Gestion de terminaux

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

1 Gérer les terminaux avec Workspace ONE UEM 5

2 Affichage en liste des terminaux 7

- Filtrage des terminaux dans l'affichage en liste 15
- Ajouter un terminal depuis l'affichage en liste 17

3 Gestion des certificats 20

4 politiques de conformité 22

- Affichage en liste des politiques de conformité 23
  - Afficher la page Mes terminaux 25
- Règles de politiques de conformité par plateforme 26
  - Descriptions des règles des politiques de conformité 27
  - Actions de politiques de conformité par plateforme 29
- Ajouter une politique de conformité 31
  - Afficher l'attribution des terminaux, stratégie de conformité 34
- Détection des terminaux compromis avec attestation d'intégrité 35
  - Configurer les politiques de conformité d'attestation d'intégrité pour Windows Desktop 36
  - Configurer des stratégies de conformité d'attestation de santé pour Windows Phone 38

5 Attributs personnalisés 40

6 Commandes effectués sur les terminaux des élèves 45

7 Attributions de terminaux 53

8 Détails du terminal 59

9 Enrôlement du terminal 63

- Enrôler un terminal auprès de Workspace ONE Intelligent Hub 64
- Flux de travail d'enrôlement supplémentaires 65
- Restrictions d'enrôlement supplémentaires 66
- Enrôlement par détection automatique 72
- Enrôlement basique vs. enrôlement par services d'annuaire 74
- Enrôlement BYOD (Bring Your Own Device) 78
- Configurer les options d'enrôlement 81
- Enregistrement des terminaux sur liste bloquée et liste autorisée 90

Enregistrement du terminal 91
État de l'enrôlement 100
Auto-enrôlement ou préenrôlement 102
Ordre de priorité des groupes organisationnels pour l'enrôlement des utilisateurs 110
Enrôlement direct de Workspace ONE 112

10 Profils du terminal 117
Traitement du profil 117
Ajouter des paramètres généraux de profil 121
Affichage en liste des profils 124
Version d'évaluation technique : profils et ressources de profil utilisés dans les workflows 129
Modification du profil du terminal 130
Profils de conformité 132
Ressources du profil 133
Ajouter une ressource Exchange 135
Ajouter une ressource Wi-Fi 139
Ajouter une ressource VPN 141
Zones de géo-barrière 145
Horaires 147
Afficher l'attribution des terminaux, profil de terminal 149

11 Balises de terminal 150

12 Valeurs de recherche 155

13 Confidentialité pour les déploiements de terminaux personnels 157

14 Ressources 171
Version d'évaluation technique : créer une fenêtre de temps et l'appliquer aux terminaux 173

15 Terminaux partagés 176

16 Protection contre la réinitialisation 184

Gérer les terminaux avec Workspace ONE UEM

1

Gérez les terminaux de votre flotte et effectuez des opérations sur un ensemble spécifique de terminaux avec Workspace ONE UEM.

Vous pouvez examiner le flux de données avec le **Monitor** et étudier de plus près votre flotte avec le **Tableau de bord des terminaux**. Vous pouvez regrouper des terminaux et créer des listes personnalisées avec **l'affichage en liste des terminaux**.

Vous pouvez également générer des **rapports** et utiliser des **balises** pour identifier facilement les terminaux. Vous pouvez même configurer le **portail en libre-service** pour permettre aux utilisateurs finaux de gérer eux-mêmes leurs terminaux et réduire ainsi la charge de travail du support technique. Pour plus d'informations, consultez Portail en libre-service dans Workspace ONE UEM.

Tableau de bord des terminaux

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

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

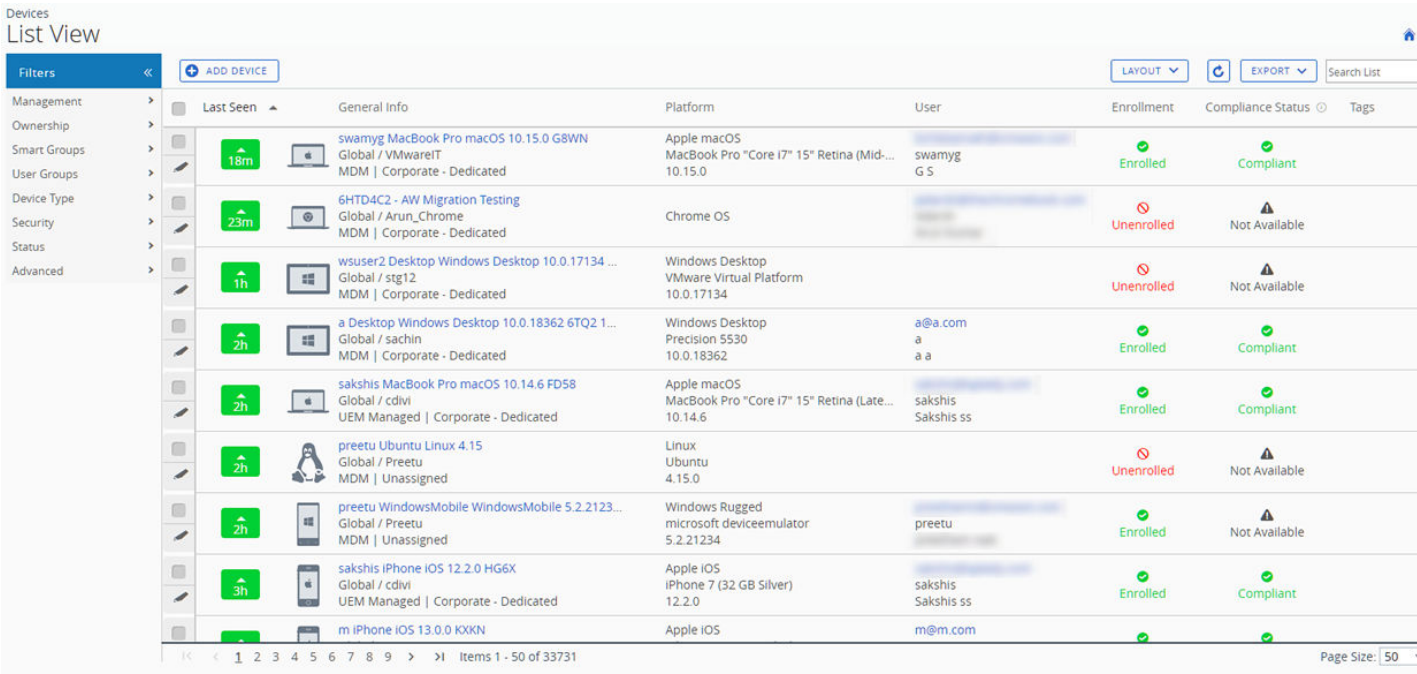
À partir de cet **affichage en liste**, vous pouvez effectuer des actions administratives : envoyer un message, verrouiller ou supprimer des terminaux et modifier les groupes associés à un terminal.

- **Sécurité** – Affichez les causes principales de problèmes de sécurité dans votre flotte de terminaux. La sélection de l'un des graphiques en anneau affiche une **liste de terminaux** filtrés qui sont concernés par le problème de sécurité sélectionné. Si elle est prise en charge par la plateforme, vous pouvez configurer une stratégie de conformité pour entreprendre des actions sur ces terminaux.
  - **Compromis** –Nombre et pourcentage de terminaux compromis (craqués) dans votre déploiement.

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

Affichage en liste des terminaux 2

Utilisez l'affichage en liste des terminaux dans Workspace ONE UEM pour afficher une liste complète des terminaux du groupe organisationnel actuellement sélectionné. Vous pouvez également filtrer la vue pour afficher uniquement les types de terminaux que vous souhaitez voir.



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

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

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

Fenêtre pop-up de pointage dans l'affichage en liste des terminaux

Chaque terminal figurant dans la colonne **Informations générales** comporte une icône d'infobulle ayant la forme d'un dossier en haut à droite, à côté du nom convivial du terminal. Lorsque vous appuyez sur cette icône (terminal mobile tactile) ou passez le curseur de la souris dessus (PC ou Mac), une fenêtre pop-up de pointage s'affiche. Cette fenêtre pop-up contient les informations suivantes : **Nom convivial**, **Groupe organisationnel**, **ID de groupe**, **Gestion** et **Propriété**.

Les colonnes **Enrôlement** et **Statut de conformité** de la vue liste des terminaux comportent des icônes avec infobulles semblables. Ces icônes avec infobulles affichent des fenêtres pop-up de pointage avec **Date d'enrôlement** et **Violation de la conformité**, respectivement.

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

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

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

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

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

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

Exporter l'affichage en liste

Vous pouvez enregistrer un fichier .xlsx ou .csv (valeurs séparées de virgules) comprenant l'intégralité de l'**Affichage en liste** et qui pourra ensuite être ouvert et analysé avec Microsoft Excel. Si un filtre est appliqué à l'**Affichage en liste du terminal**, la liste exportée sera également filtrée.

Sélectionnez le bouton **Exporter**, choisissez le format (**.xlsx** ou **.csv**), puis rendez-vous dans **Surveillance > Rapports et analyses > Exports** pour afficher et télécharger le rapport correspondant.

Recherche dans l'affichage en liste des terminaux

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

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

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

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

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

Pour obtenir la liste complète des actions à distance qu'un administrateur peut appeler à l'aide de la console, reportez-vous à la section Chapitre 6 Commandes effectués sur les terminaux des élèves.

Assistance à distance

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

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

- Vous devez posséder une licence valide pour Workspace ONE assistance.

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

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

Pour plus d'informations, reportez-vous au Guide Workspace ONE Assist.

Terminaux désenrôlés

Les terminaux désenrôlés peuvent ou non être affichés dans Workspace ONE UEM Console selon qu'ils ont été enregistrés ou qu'ils ont eu l'état Enrôlé précédemment. Vous pouvez également accéder aux journaux de dépannage créés avant le désenrôlement d'un terminal depuis UEM Console.

État désenrôlé

Un terminal désenrôlé est à l'un des trois états suivants.

1 Le terminal débute sur Workspace ONE UEM et n'est ni enrôlé, ni enregistré. Il n'est par conséquent pas géré. Un terminal à cet état est invisible dans UEM Console.

2 Le nouveau terminal a commencé le processus d'enrôlement à Workspace ONE et est enregistré auprès d'UEM Console, mais n'est pas encore tout à fait enrôlé. Normalement, ce scénario se produit durant une vague de nouveaux enrôlements au cours de laquelle les terminaux sont enregistrés pour restreindre l'enrôlement. La liste autorisée de terminaux constitue le mécanisme grâce auquel les terminaux enregistrés peuvent s'enrôler. Un terminal à cet état est visible d'UEM Console, à l'état « Désenrôlé ». Étant donné qu'un terminal enregistré fait traditionnellement partie du processus d'enrôlement, il ne reste pas à cet état très longtemps.

3 Un terminal peut également devenir désenrôlé si l'utilisateur final du terminal supprime manuellement le profil MDM de ce dernier.

Pour plus d'informations, consultez la section **Suppression de terminaux** sur cette page.

Accès aux journaux de dépannage créés avant le désenrôlement

Vous pouvez accéder à des journaux de dépannage/commandes créés avant le désenrôlement du terminal. Ces journaux peuvent être utiles pour obtenir une image complète de l'historique du terminal.

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

2 Sélectionnez un terminal désenrôlé par le passé. Vous avez la possibilité de **filtrer** l'affichage en liste pour afficher uniquement les terminaux à l'**état Désenrôlé**.

Résultat : lorsque vous sélectionnez un terminal, la vue **Affichage détaillé** s'affiche.

3 Sélectionnez le menu déroulant **Plus**, puis **Dépannage**, suivi de l'onglet **Commandes**.

Que faire ensuite ? Si vous ne prévoyez pas de ré-enrôler au même groupe organisationnel client un terminal précédemment désenrôlé, envisagez de supprimer définitivement l'enregistrement du terminal afin que l'historique de ce dernier soit vierge lors du ré-enrôlement. Contactez le support Workspace ONE réaliser cette opération.

Actions en masse dans l'affichage en liste des terminaux

Après avoir filtré un sous-ensemble de terminaux, vous pouvez effectuer des actions en masse en sélectionnant les terminaux et en sélectionnant l'un des boutons d'option.

Les actions en masse sont uniquement disponibles dans l'affichage en liste des terminaux si elles sont activées dans les paramètres système (**Groupes et paramètres > Tous les paramètres > Système > Sécurité > Actions restreintes**). La protection par mot de passe nécessite un code PIN.

Avec les terminaux sélectionnées dans l'**affichage en liste**, le nombre de terminaux sélectionnés s'affiche en regard des boutons d'actions. Ce nombre comprend des terminaux triés qui sont également sélectionnés.

Note Dans la vue de la liste des terminaux, les actions en masse disponibles lorsque vous sélectionnez un bloc de terminaux avec la touche Maj peuvent être différentes des actions en masse disponibles lorsque vous sélectionnez la case principale.

Pour plus d'informations sur les actions affectées, consultez la section Chapitre 6 Commandes effectués sur les terminaux des élèves. Pour plus d'informations sur les méthodes de sélection, consultez la section **Sélection des terminaux dans l'affichage en liste des terminaux** sur cette page.

Limite de la gestion en masse dans l'affichage en liste des terminaux

Vous pouvez définir un nombre maximum de terminaux pouvant recevoir une commande d'action en masse afin d'assurer la facilité des opérations dans le cadre d'une gestion de flotte importante.

Vous pouvez modifier ces limites en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Avancé > Gestion en masse**. Il y a plusieurs actions de terminal répertoriées pour lesquelles vous pouvez modifier le nombre maximal de terminaux autorisés.

Lorsqu'une limite de gestion en masse existe et que plusieurs terminaux sont sélectionnés, un lien apparaît en regard du message relatif au nombre d'éléments sélectionnés : **certaines actions sont désactivées en raison d'une limite de gestion en masse.** Cela signifie que le nombre de terminaux que vous avez sélectionné dépasse le nombre maximal de terminaux autorisés pour certaines actions de terminal.

Vous pouvez cliquer sur ce lien pour découvrir les actions qui ont été désactivées.

Avertissement d'actions en masse en attente dans l'affichage en liste des terminaux

L'exécution des actions en masse est longue. Lors de l'exécution d'une nouvelle action en masse (alors que l'action précédente est toujours en cours de traitement par Workspace ONE™ UEM Console), un message d'avertissement est généré.

```
Your previous bulk actions requested are still being processed. This request is run once the previous actions are complete. Do you want to continue with the current request?
```

Cliquez sur **Oui** pour ajouter la nouvelle action en masse à la file d'attente. Cliquez sur **Non** pour annuler la nouvelle action en masse.

Sélection des terminaux dans l'affichage en liste des terminaux

Vous pouvez sélectionner des terminaux individuels en cochant individuellement les cases à gauche de chaque terminal. Vous pouvez aussi sélectionner un bloc de terminaux sur plusieurs pages. Vous pouvez même sélectionner tous les terminaux de votre flotte, ce qui pourrait déclencher un avertissement sur les actions restreintes.

Sélection d'un bloc de terminaux

Vous pouvez sélectionner un bloc continu de terminaux, et ce, sur plusieurs pages si vous le souhaitez en cochant la case du terminal au début du bloc. Ensuite, maintenez la touche Maj enfoncée, puis sélectionnez la case du terminal à la fin du bloc. Cette sélection de bloc est semblable à celle des environnements Windows et Mac et vous permet d'effectuer des actions en masse sur les terminaux sélectionnés.

Sélection de tous les terminaux

La case principale située à gauche de l'en-tête de la colonne **Dernière connexion** peut être utilisée pour sélectionner ou désélectionner tous les terminaux de la liste. Si votre **affichage en liste** contient une liste filtrée de terminaux, la case principale peut être utilisée pour sélectionner ou désélectionner tous les terminaux filtrés.

Lorsque la case principale comporte un signe moins vert () signifie qu'au moins un terminal est sélectionné, mais pas tous. Sélectionnez à nouveau cette icône et elle se transforme en une coche (), indiquant que tous les terminaux de la liste (filtrés ou non filtrés) ont été sélectionnés. Sélectionnez-la une troisième fois et elle redevient une case vide (), indiquant qu'aucun terminal dans la liste n'est actuellement sélectionné.

Note Dans la vue de la liste des terminaux, les actions en masse disponibles lorsque vous sélectionnez un bloc de terminaux avec la touche Maj peuvent être différentes des actions en masse disponibles lorsque vous sélectionnez la case principale.

Pour plus d'informations sur les actions affectées, consultez la section Chapitre 6 Commandes effectués sur les terminaux des élèves.

Avertissement sur les restrictions d'une action appliquée à tous les terminaux sélectionnés

Quand un bouton d'action est activé après la sélection de tous les terminaux de votre flotte, un message d'avertissement s'affiche.

Vous essayez d'appliquer cette action à [nombre d'éléments sélectionnés] terminaux. Cette action peut ne pas s'appliquer à tous les terminaux. Certaines limites de cette action pourraient inclure le statut d'enrôlement, le type de gestion, la plateforme du terminal, le modèle ou l'OS.

Cet avertissement est lié à la diversité d'une flotte importante de terminaux représentant une multitude de fabricants, de systèmes d'exploitation et de fonctionnalités. Il est indépendant et non lié à la **limite de gestion en masse** et aux avertissements qu'elle pourrait générer. Si vous avez défini une **limite de gestion en masse**, ce **message d'avertissement sur les actions restreintes** ne s'affiche pas.

Suppression de terminaux

Vous pouvez supprimer un terminal enrôlé depuis la Workspace ONE UEM Console.

La suppression d'un terminal a trois conséquences.

1 Le terminal est retiré de l'affichage en liste des terminaux.

2 Un *effacement des données d'entreprise est exécuté, ce qui supprime du terminal tout contenu d'entreprise sensible.

3 Le terminal est ainsi exclu de toutes les fonctions et fonctionnalités de gestion des terminaux.

Cependant, un terminal supprimé est toujours enregistré dans la console UEM et est ajouté à la liste autorisée. Cet ajout signifie que le terminal supprimé peut être réenrôlé facilement. Un terminal peut rester à cet état indéfiniment. Vous pouvez conserver jusqu'à environ 150 000 terminaux sur cette liste autorisée. Contactez le support si vos besoins dépassent ce chiffre.

Vous pouvez supprimer l'enregistrement de n'importe quel terminal sur liste autorisée à tout moment, ce qui rend ce dernier invisible et inconnu de la console UEM. Un terminal dans ce scénario peut être enrôlé à une date ultérieure.

Sinon, vous pouvez supprimer le terminal de la liste autorisée et l'ajouter à une liste bloquée, ce qui empêche l'enrôlement futur et bannit efficacement le terminal de votre flotte.

Pour plus d'informations sur l'ajout sur liste autorisée ou bloquée de terminaux, consultez Enregistrement des terminaux sur liste bloquée et liste autorisée.

Vous pouvez supprimer un terminal de l'affichage en liste des terminaux ou de la vue Détails du terminal.

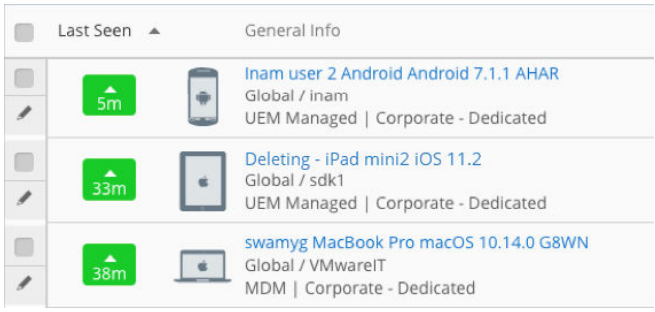
1 Accédez à **Terminaux > Affichage en liste** et sélectionnez le terminal que vous souhaitez supprimer en cochant la case située à gauche de la liste des terminaux.

   a Certains terminaux ne peuvent pas être supprimés de l'affichage en liste. Si vous souhaitez supprimer de tels terminaux, accédez à **Terminaux > Affichage en liste** et sélectionnez plutôt le **Nom convivial** du terminal dans la colonne **Informations générales**. Cette action affiche la **Vue Détails**. Le **Nom convivial** est l'étiquette que vous attribuez à un terminal pour vous aider à le différencier des terminaux de la même marque et du même modèle.

2 Localisez le bouton **Plus d'actions** et sélectionnez-le.

3 Sélectionnez **Supprimer le terminal**, puis **OK** dans l'invite de confirmation.

Résultat : l'entrée de l'affichage en liste des terminaux relative au terminal supprimé comprend l'indicateur « Suppression ».



* Lorsque vous sélectionnez plusieurs terminaux à supprimer, vous pouvez déclencher la fonctionnalité de protection contre l'effacement. Tous les terminaux effacés après l'activation de la protection contre l'effacement doivent être supprimés manuellement.

Par exemple, si vous sélectionnez 25 terminaux à supprimer et que la protection contre l'effacement est activée après 10 suppressions, les 15 terminaux restants après l'activation de la protection contre l'effacement voient leurs données d'entreprise effacées, mais ils ne sont pas supprimés d'UEM comme les 10 premiers. Vous devez supprimer manuellement ces 15 terminaux restants.

Pour plus d'informations, consultez la sectionChapitre 16 Protection contre la réinitialisation.

Ce chapitre contient les rubriques suivantes :

- Filtrage des terminaux dans l'affichage en liste
- Ajouter un terminal depuis l'affichage en liste

Filtrage des terminaux dans l'affichage en liste

Vous pouvez appliquer des filtres pour afficher uniquement les terminaux de votre choix. Sélectionnez le bouton **Filtrer** pour afficher tous les filtres suivants afin d'afficher uniquement les terminaux qui correspondent aux catégories que vous avez sélectionnées.

Spécifiez autant de filtres que vous le souhaitez. La liste des terminaux n'est pas mise à jour tant que le bouton **Appliquer** n'est pas activé*.

Paramètre	Description
Gestion	Affichez les terminaux gérés au **niveau de l'application** ou par **Catalog**, **Container** ou **MDM**. Affichez les terminaux gérés par une méthode **inconnue**, **hors ligne** ou **toutes les** méthodes de gestion.
Propriété	Affichez les terminaux possédant les niveaux de propriété **Professionnel**, **Partagé**, **Personnel** ou **Non attribué**. Vous pouvez filtrer plusieurs niveaux de propriété à la fois.
Smart Groups	Affichez les terminaux faisant partie du Smart Group que vous avez sélectionné. Cliquez sur la zone de texte de **recherche** et faites votre choix dans la liste de Smart Groups qui s'affiche. Faites défiler vers le bas pour afficher la liste des Smart Groups par ordre alphabétique.
Groupes d'utilisateurs	Affichez les terminaux faisant partie des groupes d'utilisateurs que vous avez sélectionnés. Cliquez sur la zone de texte de **recherche** et faites votre choix dans la liste de groupes d'utilisateurs qui s'affiche. Faites défiler vers le bas pour afficher la liste des groupes d'utilisateurs par ordre alphabétique.

Paramètre	Description
Type de terminal	
Plate-forme	Faites votre choix dans la liste complète de plateformes de terminal. Vous pouvez filtrer plusieurs plateformes à la fois.
Gestion des terminaux Android *	Disponible uniquement lorsque la plateforme **Android** est sélectionnée. Vous devez sélectionner au moins une plateforme et cliquer sur le bouton **Appliquer** avant de pouvoir sélectionner les types de gestion. Filtrez les types de gestion de terminaux spécifiques à la plateforme Android. Vous pouvez également activer la colonne Gestion des terminaux Android pour qu'elle s'affiche en Personnalisez l'aperçu de l'affichage en liste des terminaux. Cette colonne apparaît également dans Exporter l'affichage en liste.
Modèles de terminaux*	Vous devez sélectionner au moins une plateforme et cliquer sur le bouton **Appliquer** avant de pouvoir sélectionner des modèles de terminaux.
Version d'OS*	Vous devez sélectionner au moins une plateforme et cliquer sur le bouton **Appliquer** avant de pouvoir sélectionner les versions du système d'exploitation. Lorsque vous sélectionnez plusieurs plateformes, une liste s'affiche et présente les versions de système d'exploitation regroupées par plateforme sélectionnée.
Sécurité	
Compromis	Faites votre choix entre **Compromis**, **Non compromis**, **Inconnu** ou **Toutes** les propositions ci-dessus. Un terminal compromis a été « craqué » (pour les terminaux iOS) ou rooté (pour les terminaux Android).
Chiffrement	Faites votre choix entre **Chiffré**, **Non chiffré**, **Inconnu** ou **Toutes** les propositions ci-dessus.
Code d'accès	Faites votre choix entre **Code d'accès**, **Aucun code d'accès**, **Inconnu** ou **Toutes** les options de code d'accès.
Statut	
État de l'enrôlement	Faites votre choix entre **Enrôlé**, **En attente d'effacement des données professionnelles**, **En attente de la réinitialisation du terminal**, **Non enrôlé** ou **Toutes** les propositions ci-dessus.
Dernière connexion	Affichez les terminaux en fonction de leur date de connexion. Utilisez les zones de texte Minimum et Maximum dans l'option **Dernière connexion (en jours)** pour afficher les derniers terminaux actifs dans une plage de jours. Les numéros saisis sont inclus : une entrée de 1 affiche tous les terminaux dont la dernière connexion remonte à plus de 1 jour, mais à moins de 2 jours. Une entrée de 2 affiche tous les terminaux dont la dernière connexion remonte à plus de 2 jours, mais à moins de 3 jours, etc. Une entrée de 0 affiche les terminaux dont la dernière connexion remonte à plus de 0 jour, mais à moins de 1 jour (24 heures). Pour afficher les terminaux dont la dernière connexion est supérieure (ou égale) au nombre maximum de jours saisi, laissez la zone de texte Minimum vide. Pour afficher les terminaux dont la dernière connexion est inférieure (ou égale) au nombre minimum de jours saisi, laissez la zone de texte Maximum vide.
Politique	Faites votre choix entre **Conforme**, **Non conforme**, **En attente de vérification de conformité**, **Non disponible**, **Inconnu** ou **Toutes** les propositions ci-dessus.
Historique des enrôlements	Sélectionnez les dates d'enrôlement entre **Veille**, **Semaine précédente**, **Mois précédent** ou **Tous les** dates d'enrôlement.
Avancé	
Adresse Mac	Filtrez par adresse de contrôle d'accès média du terminal.

Paramètre	Description
Plage d'adresses IP	Filtrez les terminaux selon l'adresse IP qui leur est actuellement attribuée. Entrez les adresses IP dans les zones de texte **Début** et **Fin de la plage IP** pour afficher les terminaux qui se situent dans cette plage. L'adresse IP actuelle peut être l'une des nombreuses adresses IP associées d'un terminal, la plupart d'entre elles étant disponibles dans l'onglet Réseau de Détails du terminal.
Étiquettes	Affichez les terminaux en fonction de leurs étiquettes que vous pouvez rechercher et sélectionner depuis un menu déroulant.
Tunnel	Choisissez d'afficher tous les terminaux, uniquement ceux connectés au tunnel ou ceux qui n'y sont pas.
Conformité du contenu	Choisissez d'afficher tous les terminaux, seulement ceux pour lesquels il manque des documents requis ou seulement ceux dont le contenu obligatoire ne dispose pas de la dernière version.
Lost Mode	Affichez tous les terminaux ou seulement ceux sur lesquels le mode Perdu est activé. Applicable uniquement aux terminaux iOS.

Après avoir appliqué plusieurs filtres, vous pouvez observer le badge numérique encerclé à droite du bouton **Filtres** pour voir le nombre exact de filtres appliqués afin de générer la liste.

Vous pouvez effacer tous les filtres sélectionnés et revenir à la liste complète des terminaux en cliquant sur le X en regard du bouton **Filtrer**.

Ajouter un terminal depuis l'affichage en liste

Vous pouvez ajouter ou enregistrer un terminal incluant l'attribution utilisateur, les attributs personnalisés et l'étiquetage.

Procédure

1 Accédez à **Terminaux > Affichage en liste** ou **Terminaux > Cycle de vie > Statut d'enrôlement**.

2 Cliquez sur le bouton **Ajouter un terminal**. La page **Ajouter un terminal** s'affiche. Configurez les paramètres suivants :

Tableau 2-1. Utilisateur

Paramètre	Description
Texte recherché	Chaque terminal doit être attribué à un utilisateur. Recherchez un utilisateur dans la zone de texte en saisissant les paramètres de recherche et cliquez sur **Rechercher un utilisateur**. Vous pouvez sélectionner un utilisateur parmi les résultats de la recherche ou cliquez sur **Créer un utilisateur**.

Tableau 2-2. Créer un utilisateur

Paramètres	Description
Type de sécurité	Choisissez entre utilisateurs **basiques** et d'**annuaire**. Pour plus d'informations, reportez-vous aux rubriques Authentification basique et Authentification Active Directory.
Nom d'utilisateur	Saisissez le nom d'utilisateur qui identifie votre utilisateur dans votre environnement.

Tableau 2-2. Créer un utilisateur (suite)

Paramètres	Description
Mot de passe, **Confirmer le mot de passe**	Saisissez et confirmez le mot de passe correspondant au nom d'utilisateur.
Adresse e-mail	Saisissez l'adresse e-mail du compte utilisateur.
Groupe organisationnel d'enrôlement	Le groupe organisationnel qui sert de groupe organisationnel pour l'enrôlement du terminal.
Afficher les détails avancés de l'utilisateur	Affichez tous les détails avancés de l'utilisateur, y compris des informations détaillées concernant le nom de l'utilisateur, le numéro de téléphone de l'utilisateur et le nom du responsable. Vous trouverez également des paramètres d'identification facultatifs tels que le service, l'identifiant de l'employé et le centre de coûts. Sélectionnez le **rôle utilisateur** par défaut pour l'utilisateur que vous ajoutez, ce qui détermine les permissions dont il bénéficie lorsqu'il utilise un terminal connecté. Pour plus d'informations, reportez-vous à la rubrique Rôles utilisateur.

Tableau 2-3. Les profils de terminaux

Paramètres	Description
Nom convivial attendu	Le **nom convivial attendu** d'un terminal est l'étiquette que vous attribuez à un terminal pour vous aider à le différencier des terminaux de la même marque et du même modèle. Vous pouvez choisir un nom convivial entré manuellement ou vous pouvez incorporer des valeurs de recherche. Pour plus d'informations, reportez-vous à la section Chapitre 12 Valeurs de recherche.
Groupe organisationnel	Sélectionnez dans le menu déroulant le groupe organisationnel auquel le terminal est associé.
Propriété	Sélectionnez le type de propriété dans le menu déroulant. Choisissez entre **Aucun**, **Professionnel**, **Partagé** et **Personnel**.
Plateforme	Sélectionnez la plateforme du terminal dans le menu déroulant.
Afficher les options avancées d'informations du terminal	Affichez tous les paramètres avancés d'informations du terminal.

Tableau 2-4. Paramètres avancés d'informations du terminal

Paramètres	Description
Modèle	Sélectionnez le modèle du terminal dans le menu déroulant. Les contenus de ce menu dépendent de la sélection faite dans la liste déroulante **Plateforme**.
OS	Sélectionnez le système d'exploitation du terminal dans le menu déroulant. Les contenus de ce menu dépendent de la sélection faite dans la liste déroulante **Plateforme**.
UDID	Saisissez l'UDID du terminal
Numéro de série	Saisissez le numéro de série du terminal.
IMEI	Saisissez le numéro IMEI à 15 chiffres du terminal.

Tableau 2-4. Paramètres avancés d'informations du terminal (suite)

Paramètres	Description
SIM	Saisissez les spécifications de la carte SIM du terminal.
Numéro d'actif	Saisissez le numéro d'actif du terminal. Ce numéro est créé en interne par votre entreprise et ce paramètre est prévu pour tenir ce point de données.

Tableau 2-5. Messagerie

Paramètre	Description
Type de message	Sélectionnez le type de message que vous souhaitez envoyer (**Aucun**, **SMS** ou **E-mail**) au terminal lors de son inscription dans l'environnement.
Adresse e-mail	Saisissez l'adresse e-mail à laquelle vous voulez envoyer le message d'enrôlement. Cette zone de texte est disponible seulement lorsque E-Mail est sélectionné comme **type de message**.
Modèle d'e-mail	Sélectionnez le modèle d'e-mail dans le menu déroulant. Vous pouvez utiliser un lien pour ouvrir la page Modèle de message et créer un modèle de message de l'e-mail.
Numéro de téléphone	Saisissez le numéro de téléphone auquel vous voulez envoyer le SMS. Cette zone de texte est disponible seulement lorsque SMS est sélectionné comme **type de message**.
Modèle de SMS	Sélectionnez le modèle de SMS dans le menu déroulant. Vous pouvez utiliser un lien pour ouvrir la page Modèle de message et créer un modèle de message du SMS.

3 (Facultatif) Affectez des **attributs personnalisés** au terminal. Cliquez sur **Ajouter** et indiquez un **attribut** et sa **valeur**.

4 (Facultatif) Affectez des **étiquettes** au terminal. Cliquez sur **Ajouter** et sélectionnez une étiquette dans le menu déroulant pour chacune des étiquettes que vous souhaitez attribuer.

5 Cliquez sur **Enregistrer**.

Gestion des certificats

3

Envisagez d'implémenter des certificats numériques pour sécuriser vos ressources d'entreprise. En effet, les certificats offrent un niveau de stabilité, de sécurité et d'authentification que les mots de passe ne peuvent assurer. Workspace ONE UEM powered by AirWatch résout ce problème de garantie de la sécurité tout au long du cycle de vie d'un terminal à l'aide de certificats numériques.

Avec la normalisation de la mobilité de contenus professionnels sensibles, les risques d'accès non autorisés et de menaces malveillantes augmentent. Même si vous protégez votre messagerie, votre Wi-Fi et votre VPN d'entreprise à l'aide de mots de passe forts, votre infrastructure reste vulnérable aux attaques par force brute et par dictionnaire, ainsi qu'aux erreurs humaines.

Révoquer et renouveler des certificats numériques

Une fois les certificats numériques déployés émis, Workspace ONE UEM vous permet de les gérer à l'aide de l'**affichage en liste des certificats**. Les administrateurs peuvent afficher et trier les certificats par terminal, autorité, utilisateur, profil et date d'émission, etc. Vous pouvez révoquer et renouveler des certificats individuellement ou en masse.

L'affichage en liste des certificats résume les certificats déployés et vous permet de renouveler ou de révoquer les certificats individuellement ou en masse. Localisez et révoquez tous les certificats numériques depuis un terminal/utilisateur activé ou renouvelez/faites tourner tous les certificats d'authentification avant l'expiration de la conformité.

1 Lancez la procédure en accédant à **Terminaux > Certificats > Affichage en liste**.

2 Identifiez et sélectionnez les certificats numériques que vous voulez renouveler ou révoquer en cochant les cases vides.

3 Sélectionnez le bouton d'action de l'action que vous souhaitez appliquer aux certificats sélectionnés. Les choix sont les suivants :

- Renouvellement
- Méthode

Ressources d'intégration des certificats

Pour obtenir les détails de chacun des documents de certificat acceptés par Workspace ONE UEM, accédez à Intégration des autorités de certification.

politiques de conformité

4

Le moteur de conformité est un outil automatisé de Workspace ONE UEM powered by AirWatch qui garantit que tous les terminaux respectent les stratégies que vous définissez. Ces stratégies peuvent inclure les paramètres de sécurité de base, tels que l'utilisation obligatoire d'un code secret et l'application de certaines précautions, notamment la définition d'un code secret fort, la mise sur liste bloquée de certaines applications et la vérification obligatoire des terminaux à des intervalles définis.

Après avoir déterminé que les terminaux ne sont pas conformes, le moteur de conformité avertit l'utilisateur pour qu'il résolve les erreurs de conformité et évite une action disciplinaire sur le terminal. Par exemple, le moteur de conformité peut envoyer un message à l'utilisateur pour l'informer que son terminal n'est pas conforme.

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

Vous pouvez automatiser les escalades, en l'absence de correction : verrouillage du terminal et notification envoyée à l'utilisateur pour lui demander de vous contacter pour le déverrouiller. Ces étapes d'escalade, ces actions disciplinaires, ces périodes de grâce et ces messages sont entièrement personnalisables dans UEM Console.

Il existe deux méthodes pour tester la conformité.

- Conformité en temps réel (RTC)

  Des échantillons non programmés envoyés par le terminal sont utilisés pour déterminer si celui-ci est conforme. Les échantillons sont envoyés à la demande de l'administrateur.

- Conformité moteur

  Le moteur de conformité, un algorithme logiciel qui reçoit et mesure des échantillons planifiés, détermine principalement la conformité d'un terminal. Les intervalles de temps pour l'exécution du planificateur sont définis dans la console par l'administrateur.

L'application des stratégies de sécurité mobile fait l'objet de cette présentation générale.

1 Choisir votre plateforme.

Déterminer sur quelle plateforme vous souhaitez appliquer la conformité. Une fois qu'une plateforme est sélectionnée, les options qui s'affichent ne correspondent qu'à cette plateforme.

2 Établissez vos politiques.

Personnalisez votre politique : liste d'applications, statut de compromission, chiffrement, fabricant, modèle, version du système d'exploitation, code secret et itinérance.

3 Définissez des escalades.

Configurez des actions selon un intervalle de temps en heures ou en jours, et adoptez une approche à plusieurs niveaux pour ces actions.

4 Indiquez des actions.

Envoyez des notifications par SMS, e-mail ou transfert au terminal de l'utilisateur ou envoyez un e-mail seulement à un administrateur. Demandez une vérification du terminal, supprimez ou bloquez certains profils, installez des profils de conformité, supprimez ou bloquez des applications et effacez les données professionnelles.

5 Configurez des attributs.

Attribuez votre politique de conformité par groupe organisationnel et Smart Group, puis confirmez l'attribution par terminal.

Confirmer la santé des terminaux Windows

Les terminaux Windows vous permettent de configurer et d'analyser la santé du terminal au démarrage pour garantir que vos ressources d'entreprise sont sécurisées. Pour plus d'informations, reportez-vous à la section **Détection de terminal compromis avec attestation de santé** disponible dans la documentation **Gestion des terminaux Windows Desktop** sur docs.vmware.com.

Ce chapitre contient les rubriques suivantes :

- Affichage en liste des politiques de conformité
- Règles de politiques de conformité par plateforme
- Ajouter une politique de conformité
- Détection des terminaux compromis avec attestation d'intégrité

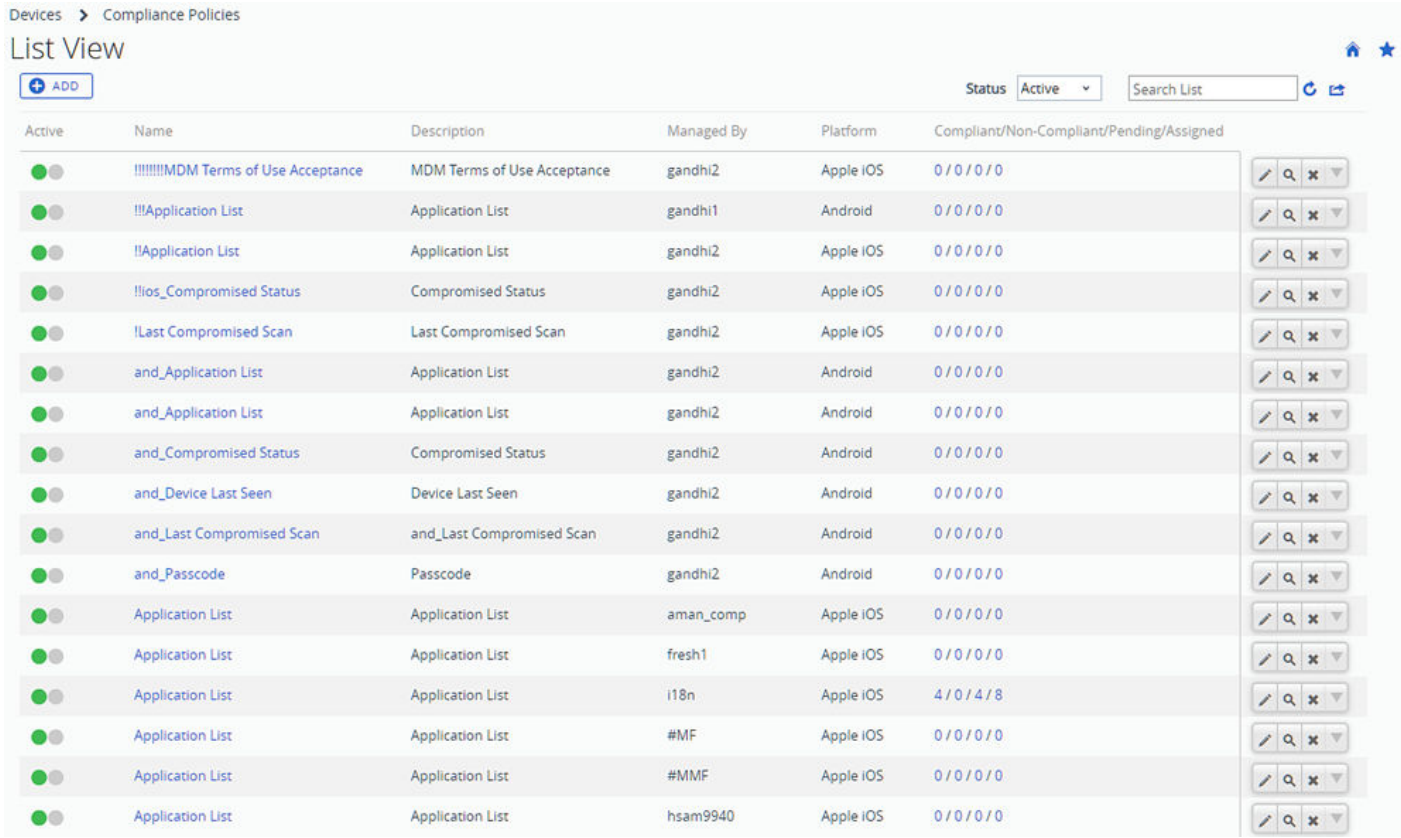
Affichage en liste des politiques de conformité

L'affichage en liste des stratégies de conformité dans Workspace ONE UEM powered by AirWatch vous permet de voir toutes les stratégies de conformité actives et inactives, ainsi que leurs configurations.

Les terminaux sont mis **en attente** de la conformité après leur premier enrôlement. La création, l'enregistrement et l'attribution d'une politique à un terminal enrôlé définiront le statut de conformité de celui-ci comme étant **conforme** ou **non conforme**.

De même, les modifications apportées aux attributions de **Smart Group** entraînent la **mise en attente** de la stratégie de conformité d'un nouveau terminal dans le Smart Group. Le statut de conformité des terminaux déjà attribués au Smart Group reste inchangé malgré l'ajout ou la suppression des attributions au Smart Group.

Visualisez l'affichage en liste des stratégies de conformité en naviguant vers **Terminaux > Stratégies de conformité > Affichage en liste**.



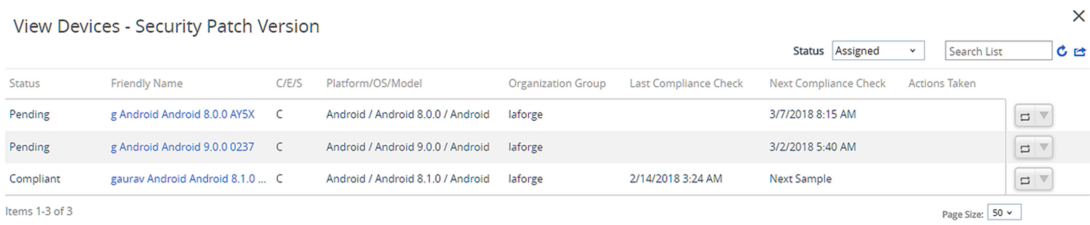
Paramètre	Description
Statut	Filtrez la liste entre les statuts **Tous/Toutes**, **Actif** et **Inactif**.
Menu d'actions 	Affichez et modifiez les politiques individuelles, affichez les terminaux auxquels la politique a été attribuée et supprimez les politiques que vous ne voulez plus conserver.

Paramètre	Description
Conforme/Non conforme/En attente/ Attribué	Les nombres de cette colonne sont des liens hypertextes qui, lorsque vous cliquez dessus, affichent la page **Afficher les terminaux** pour le statut concerné de la politique de conformité sélectionnée. Le statut **Attribué** représente le nombre de terminaux **conformes**, **non conformes** et **en attente** de vérification de la conformité. Pour plus d'informations, reportez-vous à la section Afficher la page Mes terminaux.
Bouton **Exporter**	Vous pouvez télécharger des rapports au format Excel par défaut (**.xlsx**), ou au format **.csv** (valeurs séparées de virgules), de l'affichage en liste **Stratégies de conformité**.

Afficher la page Mes terminaux

La page d'**affichage des terminaux** est utilisée pour visualiser les informations de conformité de chaque terminal attribué à la politique sélectionnée. Il s'affiche lorsque vous sélectionnez l'un des chiffres du lien hypertexte dans la colonne d'affichage de la liste de politiques de conformité **Conforme/Non conforme/En attente/Attribué**.

Filtrer la liste parmi ces quatre statuts en sélectionnant dans le menu déroulant **Statut**. Le statut **attribué** est la somme des statuts **conforme**, **non conforme** et **en attente**.



Trois statuts de conformité sont inclus dans la colonne **Statut**.

- **Conforme** – La politique de conformité attribuée a déterminé que le terminal est conforme.
- **Non conforme** – La politique de conformité attribuée a déterminé que le terminal est non conforme.
- **En attente** – La politique de conformité est en attente d'attribution au terminal nouvellement enrôlé.

Vous pouvez également vérifier la valeur **C/E/S** (propriété) du terminal, la **plateforme, le système d'exploitation ou le modèle**, le **groupe organisationnel**, la **dernière vérification de conformité**, la **prochaine vérification de conformité** et les **actions entreprises**. La colonne Actions entreprises répertorie les actions qui ont été prises pour traiter des terminaux non conformes.

Vous pouvez également choisir de réévaluer la conformité d'un terminal spécifique. Activez le moteur de conformité et resignalez l'état de conformité sur le terminal en sélectionnant **Réévaluer la conformité** ( ).

Règles de politiques de conformité par plateforme

Les règles de stratégie de conformité ne s'appliquent pas à toutes les plateformes gérées par Workspace ONE UEM powered by AirWatch. La page **Ajouter une politique de conformité** est différente selon les plateformes, si bien que vous ne pouvez voir que les règles de conformité et les actions qui s'appliquent à votre terminal.

Utilisez le tableau ci-dessous pour déterminer les règles pouvant être déployées sur vos terminaux.

Politique de conformité	Android et Android hérité	Apple iOS	Apple macOS	Chrome OS	QNX	Windows durcis	Windows 10 Desktop
Liste d'applications	✓	✓	✓				
État de l'antivirus							✓
Utilisation des données cellulaires	✓	✓					
Utilisation des SMS	✓						
Utilisation des appels	✓						
Attribut conformité							✓
Statut compromis	✓	✓					✓
Dernière connexion du terminal	✓	✓	✓	✓	✓	✓	✓
Fabricant du terminal	✓						
Chiffrement	✓	✓	✓				✓
État du pare-feu			✓				✓
Espace disponible sur le disque		✓					
Zone iBeacon		✓					
Expiration du profil de certificat interactif	✓	✓					
Dernière analyse de statut de compromission	✓	✓					
Acceptation des conditions d'utilisation MDM	✓	✓	✓			✓	✓
Modèle	✓	✓	✓				
Version du système d'exploitation	✓	✓	✓	✓			✓
Code d'accès	✓	✓					✓
Itinérance *	✓	✓					✓
Utilisation des données mobiles en itinérance *	✓	✓					

Politique de conformité	Android et Android hérité	Apple iOS	Apple macOS	Chrome OS	QNX	Windows durcis	Windows 10 Desktop
Version du correctif de sécurité	✓						
Changement de carte SIM *	✓	✓					
Protection de l'intégrité du système			✓				
Statut de mise à jour automatique sous Windows							✓
Validation d'authenticité des copies sous Windows							

Note * Disponible seulement pour les utilisateurs avancés de télécommunications.

Descriptions des règles des politiques de conformité

Les règles de conformité vous permettent de définir une base solide pour votre politique. Les actions, escalades et attributions suivantes sont établies selon ces règles.

Paramètre	Description
Liste d'applications	Repérez les applications sur liste bloquée installées sur un terminal ou celles qui ne sont pas sur liste autorisée. Vous pouvez interdire certaines applications (telles que les applications de médias sociaux) et celles ayant été mises sur liste bloquée par des fournisseurs, ou autoriser seulement les applications que vous spécifiez. En raison de la manière dont l'état des applications est signalé sur les terminaux iOS, une application n'obtient l'état « Installée » qu'une fois le processus d'installation entièrement terminé. Par conséquent, si vous créez une règle de conformité qui mesure la liste d'applications des terminaux iOS, envisagez d'appliquer une action qui évite la destruction des données. Par exemple, effacement des données d'entreprise ou effacement du contenu du terminal.
État de l'antivirus	Détectez si une application antivirus est en cours d'exécution ou non. Le moteur de stratégie de conformité surveille le centre de maintenance sur le terminal pour rechercher une solution antivirus. Windows prend en charge toutes les solutions antivirus tierces.
Utilisation des données mobiles/des SMS/des appels	Détectez les utilisateurs qui dépassent le seuil du forfait de télécommunications qui leur a été attribué. Workspace ONE UEM peut uniquement fournir une *notification* lorsque l'utilisation dépasse un seuil prédéterminé, UEM ne peut pas limiter l'utilisation réelle. Pour que cette règle de stratégie fonctionne correctement, vous devez activer le télécom **Avancé** et attribuer ce plan de télécom au terminal.
Attribut Conformité	Comparez les clés d'attribut du terminal à la sécurité des points de terminaux tiers. La valeur booléenne renvoyée représente la conformité du terminal. Disponible uniquement pour les terminaux Windows Desktop.

Paramètre	Description
Statut de compromission	Détectez si le terminal est compromis. Vous pouvez interdire l'utilisation des terminaux craqués enrôlés dans Workspace ONE UEM. Les paramètres de sécurité sont supprimés des terminaux craqués, et des programmes malveillants peuvent être introduits dans votre réseau et permettre l'accès à vos ressources d'entreprise. La surveillance du statut des terminaux compromis est particulièrement importante dans les environnements BYOD où les employés disposent de différentes versions des terminaux et différents systèmes d'exploitation.
Dernière connexion du terminal	Détectez si le terminal ne parvient pas à s'enregistrer dans le temps imparti.
Fabricant du terminal	Détectez si le fabricant du terminal vous permet d'identifier certains terminaux Android. Vous pouvez interdire ou autoriser uniquement les fabricants de votre choix.
Chiffrement	Détectez si le chiffrement est activé sur le terminal. Windows prend en charge toutes les solutions de chiffrement tierces.
Statut du pare-feu	Détectez si une application pare-feu est en cours d'exécution ou non. Le moteur de politiques de conformité vérifie le centre de maintenance sur le terminal pour définir une solution pare-feu. Windows prend en charge toutes les solutions de pare-feu tierces.
Espace disque disponible	Détectez l'espace disque disponible sur le terminal.
Zone iBeacon	Détectez si votre terminal iOS est dans la zone d'un groupe iBeacon.
Expiration du profil de certificat interactif	Détectez si un profil installé sur le terminal expire dans la période définie.
Dernière analyse de statut de compromission	Détectez si le terminal n'a pas indiqué son statut de compromission selon le planning défini.
Acceptation des conditions d'utilisation MDM	Détectez si un utilisateur n'a pas accepté les conditions d'utilisation MDM dans un certain laps de temps.
Modèle	Détectez le modèle du terminal. Vous pouvez interdire ou autoriser uniquement les fabricants de votre choix.
Version du système d'exploitation	Détectez la version du système d'exploitation. Vous pouvez interdire ou autoriser uniquement les systèmes d'exploitation et les versions de votre choix.
Code d'accès	Détectez si le terminal est protégé par un code d'accès.
Itinérance*	Détectez si le terminal est en itinérance.
Utilisation des données mobiles en itinérance*	Détecter l'utilisation des données cellulaires en itinérance contre une quantité statique de données mesurées en Mo ou en Go.
Version du correctif de sécurité	Détectez la date du dernier correctif de Google pour les terminaux Android. Applicable uniquement à Android version 6.0 et versions ultérieures.
Changement de carte SIM*	Détectez si la carte SIM a été remplacée.
Protection de l'intégrité du système	Détectez l'état de la protection propriétaire de macOS des fichiers et des répertoires appartenant au système par rapport aux modifications effectuées par des processus sans « droit d'accès » spécifique, même lorsqu'ils sont exécutés par l'utilisateur racine ou un utilisateur disposant de privilèges racine.

Paramètre	Description
Statut de mise à jour automatique sous Windows	Détectez si la mise à jour automatique sous Windows est activée. Le moteur de stratégie de conformité surveille le centre de maintenance sur le terminal pour rechercher une solution de mise à jour. Si votre solution tierce ne s'affiche pas dans le centre de maintenance, elle est signalée comme non surveillée.
Validation d'authenticité de la copie Windows Validation d'authenticité de la copie Windows	Détectez si la version Windows utilisée actuellement est authentique.

* Disponible seulement pour les utilisateurs avancés de télécommunications.

Actions de politiques de conformité par plateforme

Les actions prises en charge par plateforme, exécutées par les politiques de conformité, se présentent comme suit :

Tableau 4-1. Win32

Action des politiques de conformité	Android et Android hérité	Apple iOS	Apple macOS	Chrome OS	QNX	Windows durcis	Windows Desktop
Bloquer/supprimer toutes les applications gérées	✓	✓	✓				✓
Bloquer/supprimer toutes les applications gérées	✓	✓	✓				✓

Tableau 4-2. Commande

Action des politiques de conformité	Android et Android hérité	Apple iOS	Apple macOS	Chrome OS	QNX	Windows durcis	Windows Desktop
Modifier les paramètres d'itinérance.		✓(iOS 5 et versions ultérieures)					
Effacement des données d'entreprise***	✓	✓	✓		✓		✓
Réinitialisation des données d'entreprise	✓					✓	
Mises à jour de l'OS ****		✓					
Exiger le check-in du terminal		✓					✓
Révoquer les jetons Azure*.	✓	✓					

Tableau 4-3. E-mail

Action des politiques de conformité	Android et Android hérité	Apple iOS	Apple macOS	Chrome OS	QNX	Windows durcis	Windows Desktop
Bloquer la messagerie	✓	✓					

Tableau 4-4. Notification

Action des politiques de conformité	Android et Android hérité	Apple iOS	Apple macOS	Chrome OS	QNX	Windows durcis	Windows Desktop
Envoyer un e-mail à l'utilisateur**.	✓	✓	✓	✓		✓	✓
Envoyer un SMS au terminal.	✓	✓					✓
Envoyer une notification Push au terminal.	✓	✓	✓	✓			✓
Envoyer un e-mail à l'administrateur.	✓	✓	✓		✓	✓	✓

Tableau 4-5. Profil

Action des politiques de conformité	Android et Android hérité	Apple iOS	Apple macOS	Chrome OS	QNX	Windows durcis	Windows Desktop
Installer le Profils de conformité	✓	✓	✓				✓
Bloquer/supprimer le profil	✓	✓	✓				✓
Bloquer/supprimer le type de profil	✓	✓	✓				
Bloquer/supprimer tous les profils***	✓	✓	✓				✓

* Nécessite d'activer l'option Utiliser Azure AD pour les services d'identité dans **Paramètres > Système > Intégration d'entreprise > Services d'annuaire > Paramètres avancés**. Affecte tous les terminaux pour un utilisateur donné, désactivant ainsi toute application qui repose sur le jeton Azure.

** Inclut la possibilité d'ajouter en Cc le responsable de l'utilisateur.

*** Ces actions empêchent la distribution des profils tant que le terminal ne renvoie pas un état conforme.

**** Vous pouvez mettre à jour le système d'exploitation (OS) des terminaux disposant des versions d'iOS allant de la version 9 à la version 10.2.1 s'ils sont supervisés et enrôlés dans le DEP. Les terminaux disposant de la version iOS 10.3 ou ultérieure doivent uniquement être supervisés.

Ajouter une politique de conformité

L'ajout d'une stratégie de conformité est un processus comprenant quatre segments : Règles, Actions, Attribution et Résumé. Workspace ONE UEM powered by AirWatch se base sur le choix initial de la plateforme pour déterminer toutes les options spécifiques à la plateforme, ainsi la console ne proposera jamais une option que votre terminal ne pourra pas utiliser.

Note La conformité des terminaux durcis Windows est seulement prise en charge pour les terminaux Motorola (l'action Réinitialisation entreprise applique cette conformité).

Configurez le moteur de conformité avec des profils et des escalades automatisées en suivant les onglets de politique de conformité.

Procédure

1 Accédez à **Terminaux > Stratégies de conformité > Affichage en liste**, puis sélectionnez **Ajouter**.

2 Sélectionnez une plateforme depuis la page **Ajouter une politique de conformité** sur laquelle vous souhaitez baser votre politique de conformité.

3 Détectez les conditions en configurant l'onglet **Règles** en appliquant **Une** règle ou **Toutes** les règles.

- **Ajouter une règle** – À sélectionner pour ajouter des règles et des paramètres supplémentaires. Pour plus d'informations, consultez les sections Règles de politiques de conformité par plateforme et Descriptions des règles des politiques de conformité.
- **Précédent** et **Suivant** – À sélectionner pour revenir à l'étape précédente ou avancer vers la suivante, respectivement.

4 Définissez les conséquences en cas de non-conformité avec votre politique en complétant l'onglet **Actions**.

Les actions disponibles dépendent des plateformes. Certaines actions ne permettent pas de recevoir de profils tant qu'un état conforme n'a pas été signalé en retour. Pour plus d'informations, consultez la section Actions de politiques de conformité par plateforme.

5 Indiquez les **actions** et les **intensifications** à entreprendre.

Une **escalade** est une action automatique effectuée lorsque l'utilisateur du terminal ne prend aucune mesure pour rendre son terminal conforme suite à l'**action** précédente.

Sélectionnez les options et les types d'action à effectuer.

Tableau 4-6. Actions et escalades

Paramètre	Description
Case **Marquer comme non conforme**	La case Marquer comme non conforme permet d'effectuer des actions sur un terminal sans le marquer comme non conforme. Le moteur de conformité effectue cette tâche en respectant les règles suivantes. ■ L'option Marquer comme non conforme est activée (case cochée) par défaut pour toute action nouvellement ajoutée. ■ Si une seule case Marquer comme non conforme est activée (cochée), toutes les cases des actions et intensifications suivantes seront également marquées comme non conforme (cochées). Les cases à cocher suivantes ne peuvent pas être modifiées. ■ Si la case Marquer comme non conforme d'une action est décochée, la case de l'action/intensification suivante est alors activée (cochée) par défaut. Cette case à cocher peut être modifiée. ■ Si l'option Marquer comme non conforme d'une action/escalade est désactivée et que l'appareil respecte la règle de conformité, l'appareil est officiellement « conforme ». L'action prescrite est alors exécutée. ■ Le statut d'un terminal reste « conforme » à moins qu'il ne rencontre une action/escalade dont la case Marquer comme non conforme est activée. Le terminal est considéré à ce moment-là comme non conforme.
Application	Bloquez ou supprimez une application gérée. Vous pouvez exécuter la conformité d'applications en établissant des listes autorisées et bloquées, ou une liste d'applications requises.
Commande	Effectuez un check-in du terminal ou un effacement des données d'entreprise.
E-mail	Empêchez l'utilisateur d'utiliser les e-mails. Si vous utilisez la gestion d'e-mails avec le moteur de conformité d'e-mails, l'action « Bloquer les e-mails » s'applique. Accédez à cette option en naviguant vers **E-mail > Stratégies de conformité > Stratégies d'e-mails**. Cette action vous permet d'utiliser les politiques de conformité des terminaux, comme les listes d'applications bloquées, en plus des politiques du moteur de conformité des e-mails que vous configurez. En sélectionnant cette action, la conformité des e-mails est déclenchée grâce à une seule mise à jour de la politique du terminal, si le terminal devient non conforme.

Tableau 4-6. Actions et escalades (suite)

Paramètre	Description
Notifier	Permet d'informer quelqu'un sur la violation de la conformité. Vous avez les options suivantes pour envoyer une notification. ■ Envoyer un e-mail à l'utilisateur. ■ Envoyer un SMS* au terminal. ■ Envoyer une notification Push au terminal. ■ Envoyer un e-mail à l'administrateur. Plusieurs adresses e-mail peuvent être insérées dans le champ **Cc** à condition qu'elles soient séparées par des virgules. Vous pouvez également mettre le responsable de l'utilisateur en copie en insérant une valeur de recherche ; cliquez sur le signe plus en regard du champ Cc et sélectionnez {UsersManager} dans le menu déroulant. Pour plus d'informations, reportez-vous à la section Chapitre 12 Valeurs de recherche. Pour toutes les actions Notifier, vous avez la possibilité d'utiliser un modèle de message. Utilisez cette option en décochant la case **Modèle par défaut** ; cette dernière affiche un menu déroulant vous permettant de sélectionner un modèle de message. Il existe également un lien qui, une fois sélectionné, affiche la page **Modèle de message** dans une nouvelle fenêtre. Cette page vous permet de créer votre propre modèle de message. * Pour que les notifications SMS fonctionnent avec votre flotte de terminaux, vous devez avoir un compte auprès d'un fournisseur de passerelle tiers et configurer les paramètres de passerelle. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > SMS** et renseignez les options décrites dans Paramètres des SMS.
Profil	Installez, supprimez ou bloquez un profil de terminal, un type de profil de terminal ou un profil de conformité spécifique. Les profils de conformité sont créés et enregistrés comme les profils de terminaux Auto et Facultatif. Accédez à **Ressources > Profils et lignes de base > Profils**, puis sélectionnez **Ajouter** et **Ajouter un profil**. Sélectionnez une plateforme et, dans l'onglet de profil **Général**, sélectionnez Conformité dans le paramètre déroulant **Type d'attribution**. Les profils de conformité ne sont appliqués que dans l'onglet **Actions** sur la page **Ajouter une politique de conformité** et sont utilisés lorsqu'un utilisateur enfreint une politique de conformité. Sélectionnez **Installer le profil de conformité** depuis le menu déroulant, puis sélectionnez le profil de la conformité enregistré précédemment.

Tableau 4-7. Escalades uniquement

Paramètre	Description
Bouton **Ajouter une escalade**	Crée une escalade. Lorsque vous ajoutez des intensifications, il est préférable d'augmenter la sécurité des actions.
Après un intervalle de temps...	Vous pouvez retarder l'escalade de quelques minutes, heures ou jours.
...**procéder aux actions suivantes**	**Répéter** – Cochez cette case pour répéter l'escalade un certain nombre de fois avant l'exécution programmée de la prochaine action.

Pour macOS, vous pouvez seulement effectuer les actions suivantes :

- Réinitialisation du terminal
- Envoyer un e-mail à l'administrateur

- Effacement des données professionnelles
- Bloquer/supprimer le profil
- Envoyer un e-mail à l'utilisateur
- Bloquer/supprimer le type de profil
- Envoyer une notification Push au terminal
- Bloquer/supprimer tous les profils

6 Déterminez les terminaux qui sont soumis à la stratégie de conformité (et sont exclus de celle-ci) en renseignant les onglets **Attribution** et **Résumé** de la page Ajouter une stratégie de conformité. Nommez, finalisez et activez la stratégie sur l'onglet Résumé.

Paramètre	Description
Géré par	Sélectionnez le groupe organisationnel qui est géré par cette politique de conformité.
Groupes attribués	Attribuez un ou plusieurs groupes à cette politique. Pour plus d'informations, reportez-vous à la rubrique Groupes d'attribution.
Exclusions	Si vous souhaitez exclure des groupes, sélectionnez **Oui**. Sélectionnez ensuite l'un des groupes disponibles répertoriés dans la zone de texte **Groupes exclus**. Pour plus d'informations, reportez-vous à la rubrique **Exclure des groupes dans les profils et politiques de conformité**.
Bouton **Afficher l'attribution des terminaux**	Visualisez la liste des terminaux concernés par l'attribution de cette politique de conformité.

Même s'il s'agit d'un critère au sein d'un Smart Group, la plateforme configurée dans le profil de terminal ou la politique de conformité sera toujours prioritaire sur celle du Smart Group. Par exemple, si un profil de terminal est créé pour la plateforme iOS, il sera seulement attribué aux terminaux iOS même si le Smart Group comporte des terminaux Android.

7 Une fois que l'attribution de cette politique est terminée, cliquez sur **Suivant**.

L'onglet **Résumé** apparaît.

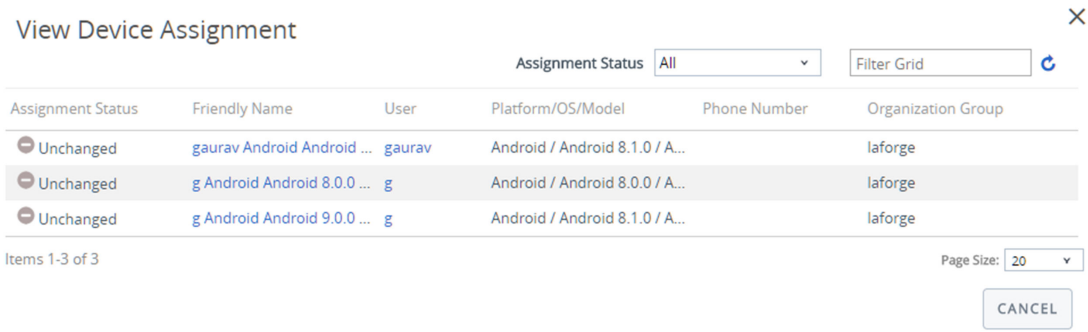
8 Fournissez un **nom** et une **description** pertinente de la politique de conformité.

9 Sélectionnez l'une des options suivantes.

- **Terminer** – Enregistrez votre politique de conformité pour les terminaux attribués sans l'activer.
- **Terminer et activer** – Enregistrez et appliquez la politique à tous les terminaux concernés.

Afficher l'attribution des terminaux, stratégie de conformité

Sélectionnez l'option **Afficher l'attribution des terminaux** dans l'onglet **Attribution** tout en configurant une politique de conformité pour afficher la page **Afficher l'attribution des terminaux**. Cette page contient les terminaux affectés (ou non affectés) par la stratégie de conformité attribuée.



La colonne **Statut de l'attribution** affiche les entrées suivantes pour les terminaux figurant dans la liste :

- **Ajouté** – La politique de conformité a été ajoutée au terminal listé.
- **Supprimé** – La politique de conformité a été supprimé du terminal.
- **Inchangé** – Le terminal n'est pas affecté par les modifications apportées à la politique de conformité.

Cliquez sur **Publier** pour finaliser les modifications et, si nécessaire, republiez toutes les politiques de conformité.

Détection des terminaux compromis avec attestation d'intégrité

L'attestation d'intégrité analyse les terminaux au démarrage et y recherche toute défaillance d'intégrité. Utilisez l'attestation de santé pour détecter les terminaux Windows Desktop compromis lorsqu'ils sont gérés sous Workspace ONE UEM powered by AirWatch.

Dans les déploiements de terminaux personnels ou appartenant à l'entreprise, il est important de savoir que les terminaux qui accèdent aux ressources de l'entreprise sont intègres. Le service d'attestation d'intégrité de Windows accède aux informations de démarrage des terminaux depuis le Cloud par l'intermédiaire de communications sécurisées. Il mesure ces informations et les compare aux points de données connexes afin de garantir que le terminal a bien démarré comme prévu et n'est pas victime de menaces ou de vulnérabilités en matière de sécurité. Les mesures comprennent le démarrage sécurisé, l'intégrité du code, BitLocker et le gestionnaire de démarrage.

Workspace ONE UEM vous permet de configurer le service d'attestation d'intégrité de Windows pour garantir la conformité des terminaux. Si l'une des vérifications activées échoue, le moteur de politique de conformité de Workspace ONE UEM applique les mesures de sécurité en fonction de la politique de conformité configurée. Cette fonction permet de garantir la protection des données de l'entreprise sur les terminaux compromis. Étant donné que Workspace ONE UEM tire les informations requises du matériel du terminal, et non de l'OS, les terminaux compromis sont détectés au moment où le noyau d'OS est compromis.

Configurer les politiques de conformité d'attestation d'intégrité pour Windows Desktop

Sécurisez vos terminaux à l'aide du service d'attestation d'intégrité de Windows pour la détection des terminaux compromis. Ce service permet à Workspace ONE UEM de vérifier l'intégrité du terminal pendant le démarrage et d'entreprendre des actions correctives.

Procédure

1. Naviguez vers **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Windows > Windows Desktop > Attestation d'intégrité Windows**.
2. (Facultatif) Sélectionnez **Utiliser le serveur personnalisé** si vous utilisez un serveur sur site personnalisé qui exécute l'attestation d'intégrité. Saisissez l' **URL du serveur**.
3. Configurez les paramètres d'attestation d'intégrité :

Paramètres	Descriptions
Utiliser le serveur personnalisé	Sélectionnez cette option pour configurer un serveur personnalisé pour l'attestation d'intégrité. Cette option nécessite un serveur exécutant Windows Server 2016 ou une version plus récente. L'activation de cette option affiche le champ URL de serveur.
URL de serveur	Saisissez l'URL de votre serveur d'attestation d'intégrité personnalisé.
Démarrage sécurisé désactivé	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le démarrage sécurisé est désactivé sur le terminal. Le démarrage sécurisé contraint le système de démarrer à un état d'usine approuvé. Lorsque le démarrage sécurisé est activé, les composants essentiels utilisés pour démarrer l'ordinateur doivent avoir les signatures cryptographiques correctes approuvées par l'OEM. Le firmware UEFI vérifie la fiabilité avant d'autoriser le démarrage de l'ordinateur. Le démarrage sécurisé bloque le démarrage s'il détecte des fichiers compromis.
Clé d'attestation d'identité (AIK) introuvable	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la clé d'attestation d'identité ne figure pas sur le terminal. Lorsqu'une clé d'attestation d'identité est présente sur un terminal, cela signifie que le terminal dispose d'un certificat EK (Endorsement Key). Il est plus fiable qu'un terminal ne disposant pas de certificat EK.

Paramètres	Descriptions
Politique de prévention de l'exécution des données (DEP) désactivée	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la politique de prévention de l'exécution est désactivée sur le terminal. La politique de prévention de l'exécution (DEP) est une fonction de protection de la mémoire intégrée au niveau système de l'OS. Cette politique empêche d'exécuter du code à partir de pages de données telles que les des segments de mémoire par défaut, des piles et des pools de mémoire. L'application de la politique DEP est un processus à la fois logiciel et matériel.
BitLocker désactivé	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le chiffrement BitLocker est désactivé sur le terminal.
Vérification de l'intégrité du code désactivée	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la vérification de l'intégrité est désactivée sur le terminal. L'intégrité du code est une fonction qui valide l'intégrité d'un pilote ou d'un fichier système chaque fois qu'il est chargé en mémoire. L'intégrité du code détecte si un fichier système ou un pilote non signés sont chargés dans le noyau. Elle détecte également si des fichiers système ont été modifiés par un logiciel malveillant exécuté par un utilisateur disposant de droits administrateur.
Logiciel anti-programme malveillant à lancement anticipé désactivé	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le logiciel anti-programme malveillant à lancement anticipé est désactivé sur le terminal. La protection contre les programmes malveillants à lancement anticipé sécurise les ordinateurs de votre réseau au démarrage et avant que les pilotes tiers ne procèdent à l'initialisation.
Vérification de la version d'intégrité du code	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la vérification de la version d'intégrité du code est un échec.
Vérification de la version du gestionnaire de démarrage	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la vérification de la version du gestionnaire de démarrage est un échec.
Vérification du numéro de version de sécurité pour l'application de démarrage	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le numéro de version de sécurité de l'application d'amorçage est différente du numéro saisi.
Vérification du numéro de version de sécurité pour le gestionnaire de démarrage	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le numéro de version de sécurité du gestionnaire d'amorçage est différente du numéro saisi.
Paramètres avancés	Activez ce paramètre pour configurer les paramètres avancés dans la section Identifiants de version logicielle.

4 Cliquez sur **Enregistrer**.

Configurer des stratégies de conformité d'attestation de santé pour Windows Phone

Sécurisez vos terminaux à l'aide du service d'attestation d'intégrité de Windows pour la détection des terminaux compromis. Ce service permet à AirWatch de surveiller l'intégrité du terminal pendant le démarrage et d'entreprendre des actions correctives.

La stratégie de conformité de l'état de compromission s'applique aux terminaux mobiles Windows 10 avec un module de plateforme sécurisée (TPM) version 1.2 ou ultérieure.

Procédure

1 Naviguez vers **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Windows > Windows Phone > Attestation de santé Windows**.

2 (Facultatif) Sélectionnez **Utiliser le serveur personnalisé** si vous utilisez un serveur sur site personnalisé qui exécute l'attestation d'intégrité. Saisissez l' **URL du serveur**.

3 Configurez les paramètres d'attestation d'intégrité :

Tableau 4-8. Définition du statut de compromission

Paramètres	Descriptions
Utiliser le serveur personnalisé	Sélectionnez cette option pour configurer un serveur personnalisé pour l'attestation d'intégrité. Cette option nécessite un serveur exécutant Windows Server 2016 ou une version plus récente. L'activation de cette option affiche le champ **URL de serveur**.
URL du serveur	Saisissez l'URL de votre serveur d'attestation d'intégrité personnalisé.
Démarrage sécurisé désactivé	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le démarrage sécurisé est désactivé sur le terminal. Le démarrage sécurisé contraint le système de démarrer à un état d'usine approuvé. Lorsque le démarrage sécurisé est activé, les composants essentiels utilisés pour démarrer l'ordinateur doivent avoir les signatures cryptographiques correctes approuvées par l'OEM. Le firmware UEFI vérifie la fiabilité avant d'autoriser le démarrage de l'ordinateur. Le démarrage sécurisé bloque le démarrage s'il détecte des fichiers compromis.
Clé d'attestation d'identité (AIK) introuvable	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la clé d'attestation d'identité ne figure pas sur le terminal. Lorsqu'une clé d'attestation d'identité est présente sur un terminal, cela signifie que le terminal dispose d'un certificat EK (Endorsement Key). Il est plus fiable qu'un terminal ne disposant pas de certificat EK.
Politique de prévention de l'exécution des données (DEP) désactivée	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la politique de prévention de l'exécution est désactivée sur le terminal. La politique de prévention de l'exécution (DEP) est une fonction de protection de la mémoire intégrée au niveau système de l'OS. Cette politique empêche d'exécuter du code à partir de pages de données telles que les des segments de mémoire par défaut, des piles et des pools de mémoire. L'application de la politique DEP est un processus à la fois logiciel et matériel.
BitLocker désactivé	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le chiffrement BitLocker est désactivé sur le terminal.

Tableau 4-8. Définition du statut de compromission (suite)

Paramètres	Descriptions
Vérification de l'intégrité du code désactivée	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la vérification de l'intégrité est désactivée sur le terminal. L'intégrité du code est une fonction qui valide l'intégrité d'un pilote ou d'un fichier système chaque fois qu'il est chargé en mémoire. L'intégrité du code détecte si un fichier système ou un pilote non signés sont chargés dans le noyau. Elle détecte également si des fichiers système ont été modifiés par un logiciel malveillant exécuté par un utilisateur disposant de droits administrateur.
Logiciel anti-programme malveillant à lancement anticipé désactivé	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le logiciel anti-programme malveillant à lancement anticipé est désactivé sur le terminal. La protection contre les programmes malveillants à lancement anticipé sécurise les ordinateurs de votre réseau au démarrage et avant que les pilotes tiers ne procèdent à l'initialisation.
Vérification de la version d'intégrité du code	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la vérification de la version d'intégrité du code est un échec.
Vérification de la version du gestionnaire de démarrage	Activez ce paramètre pour signaler un statut de terminal compromis lorsque la vérification de la version du gestionnaire de démarrage est un échec.
Vérification du numéro de version de sécurité pour l'application de démarrage	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le numéro de version de sécurité de l'application d'amorçage est différente du numéro saisi.
Vérification du numéro de version de sécurité pour le gestionnaire de démarrage	Activez ce paramètre pour signaler un statut de terminal compromis lorsque le numéro de version de sécurité du gestionnaire d'amorçage est différente du numéro saisi.
Paramètres avancés	Activez ce paramètre pour configurer les paramètres avancés dans la section Identifiants de version logicielle.

Étape suivante

Pour plus d'informations, consultez l'article de Microsoft TechNet sur l'attestation de santé.

Attributs personnalisés

5

Dans Workspace ONE UEM, les attributs personnalisés vous permettent d'extraire des valeurs spécifiques d'un terminal géré (par exemple l'IMEI ou l'emplacement, parmi d'autres) et de les utiliser comme critères d'attribution pour les produits. Vous pouvez également configurer une application tierce pour créer des attributs personnalisés et les afficher sur le lanceur.

Qu'est-ce qu'un attribut personnalisé ?

Un attribut personnalisé est un espace réservé pour les informations supplémentaires sur le terminal collectées par Workspace ONE Intelligent Hub ou par une application tierce. Cet espace réservé peut être utilisé de plusieurs manières différentes.

- Il peut être utilisé pour attribuer du contenu tel que des produits provisionnés.
  - *... par exemple, vous pouvez provisionner le produit XYZ sur les terminaux qui sont extraits et dans le champ uniquement.*
- Vous fournissez ainsi des informations à l'administrateur sur la console UEM ou à l'utilisateur final sur le terminal.
  - *... par exemple, un pilote de livraison peut afficher une application développée en interne pour déterminer son prochain arrêt, alimenté par un attribut personnalisé qui collecte l'emplacement du terminal.*
- Il peut être utilisé pour transférer des terminaux nouvellement enrôlés vers un groupe organisationnel spécifique.
  - *... par exemple, vous pouvez transférer tous les nouveaux terminaux enrôlés dont le numéro de modèle équivaut à Zebra VC80 à un groupe organisationnel qui est conçu pour répondre à ce modèle spécifique.*

Note les attributs personnalisés (et le générateur de règles) peuvent être configurés et utilisés au niveau des groupes organisationnels clients uniquement.

Pour plus d'informations sur les options disponibles concernant les règles d'attribution de terminal basées sur des attributs personnalisés, consultez la section Activer l'attribution de terminaux.

Créer un attribut personnalisé

Créez des valeurs et des attributs personnalisés à envoyer aux terminaux dans Workspace ONE UEM. Vous pouvez créer des règles d'attribution pour les produits à provisionner en fonction de ces attributs et de leurs valeurs.

1 Accédez à **Terminaux > Provisionnement > Attributs personnalisés**.

2 Cliquez sur **Ajouter**, puis **Ajouter un attribut**.

3 Dans l'onglet **Paramètres**, saisissez un **nom d'atttribut**.

4 Faites une **description** de l'attribut (facultatif).

5 Indiquez le nom de l'**application** qui regroupe l'attribut. L'application peut être une application tierce ou Workspace ONE Intelligent Hub.

6 Cliquez sur **Collecter les valeurs pour le générateur de règles** pour rendre les valeurs de l'attribut disponibles dans le menu déroulant du générateur de règles.

7 Sélectionnez **Utiliser dans le générateur de règles** si vous souhaitez utiliser l'attribut dans le générateur de règles.

8 Sélectionnez **Conserver** pour empêcher la suppression de l'attribut personnalisé de Workspace ONE UEM Console, à moins qu'un administrateur ou un appel d'API le supprime explicitement.

   Sinon, l'attribut est supprimé normalement. Si vous supprimez un attribut personnalisé signalé depuis un terminal vers UEM Console, un attribut personnalisé persistant reste dans la console. La persistance des attributs personnalisés n'est disponible que pour les terminaux durcis Windows et Android.

9 Sélectionnez l'option **Utiliser comme valeur de recherche** pour utiliser l'attribut personnalisé comme valeur de recherche où que vous vouliez dans UEM Console.

   Exemple : vous pouvez utiliser les attributs personnalisés comme faisant partie du nom convivial du terminal afin d'en simplifier la dénomination.

10 Sélectionnez l'onglet **Valeurs**.

11 Sélectionnez **Ajouter une valeur** pour ajouter des valeurs à l'attribut personnalisé.

   Vous n'avez pas besoin d'entrer toutes les valeurs possibles de l'attribut. La liste des attributs entrés ici n'est pas une exigence ou une contrainte pour les valeurs que le terminal *peut* signaler. Au lieu de cela, entrez uniquement les valeurs attendues utilisées pour prédéfinir des règles d'attribution du groupe organisationnel.

12 Cliquez sur **Enregistrer**.

Base de données des attributs personnalisés

Les attributs personnalisés sont stockés sous forme de fichiers XML et dans la base de données Workspace ONE Intelligent Hub, chacun étant stocké sur le terminal. Avec la base de données, les attributs personnalisés sont régulièrement envoyés comme échantillons à Workspace ONE UEM pour le suivi d'actifs des paires clé/valeur.

Si un enregistrement de la base de données du terminal est configuré avec la condition « Create Attribute » = TRUE, Workspace ONE Intelligent Hub récupère automatiquement le nom et la valeur envoyés avec les échantillons d'attributs personnalisés. La paire clé/valeur s'affiche sur la page Détails du terminal dans l'onglet Attributs personnalisés.

Note Les valeurs d'attribut personnalisées ne peuvent pas renvoyer les caractères spéciaux suivants : **/ \ " * : ; <> ? |**. Si un script renvoie une valeur qui contient ces caractères, la valeur n'est pas signalée sur la console. Supprimez ces caractères dans la sortie du script.

Attribuer des groupes organisationnels avec les attributs personnalisés

Configurez des règles contrôlant l'attribution de terminaux aux groupes organisationnels après l'enrôlement dans Workspace ONE UEM. Vous êtes limité à une règle d'attribution d'attributs personnalisés par groupe organisationnel.

1 Vérifiez que vous vous trouvez actuellement dans un groupe organisationnel de type Client.

2 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Avancé**.

3 Définissez l'option **Règles d'attribution des terminaux** sur **Activé**.

4 Définissez le **type** sur **Groupe organisationnel par attribut personnalisé**.

   Pour plus d'informations sur les options disponibles concernant les règles d'attribution de terminal, consultez la section Activer l'attribution de terminaux.

5 Cliquez sur **Enregistrer**.

6 Accédez à **Terminaux > Provisionnement > Attributs personnalisés > Ajouter > Ajouter un attribut** et créez un attribut personnalisé si vous ne l'avez pas encore fait.

   Consultez la section **Créer un attribut personnalisé** sur cette page.

7 Accédez à **Terminaux > Provisionnement > Attributs personnalisés > Règles d'attribution > Ajouter une règle**.

8 Sélectionnez le **groupe organisationnel** auquel la règle attribue les terminaux.

9 Cliquez sur **Ajouter une règle** pour en configurer la logique.

Paramètre	Description
Attribut/Application	Cet attribut personnalisé détermine l'attribution des terminaux. Sélectionnez entre le modèle de terminal, le numéro de série et tout attribut personnalisé ou fichier XML disponible dans le groupe organisationnel client dans lequel vous vous trouvez.
Opérateur	Cet opérateur compare l'**attribut** à la **valeur** pour savoir si le terminal remplit les conditions requises du produit. Lorsque vous utilisez plus d'un opérateur, vous devez inclure un **opérateur logique** entre chaque **opérateur**. **Note** Lorsque vous créez une règle d'attribution, les comparaisons utilisant les opérateurs inférieur à (<) et supérieur à (>) (et leurs variantes) ne peuvent être utilisées que pour comparer des valeurs numériques, y compris des entiers. L'exception se produit lorsque vous comparez des versions d'OEM Build, vous pouvez appliquer des opérateurs <et> sur des chaînes ASCII non numériques. Par exemple, lorsqu'un nom de fichier de mise à jour OEM inclut des traits d'union, des points et d'autres caractères en même temps que des chiffres. Ces règles d'attribution doivent identifier le fabricant du terminal dans la logique de la règle et cette comparaison est considérée comme exacte lorsque le format du terminal correspond à celui spécifié sur le serveur.
Valeur	Toutes les valeurs des terminaux applicables sont listées ici pour l'**attribut** sélectionné.
Ajouter un opérateur logique	Affichez un menu déroulant d'opérateurs logiques comprenant ET, OU, AUCUN, ainsi que des parenthèses. Autorisez des règles complexes.

10 Cliquez sur **Enregistrer** après avoir configuré la logique de la règle.

Résultat : lorsqu'un terminal avec un attribut personnalisé est enrôlé, la règle attribue le terminal au groupe organisationnel configuré.

Importation d'attributs personnalisés

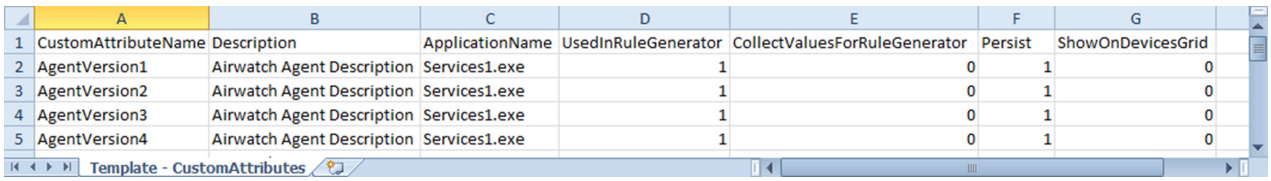
La fonctionnalité d'importation par lot des attributs personnalisés de Workspace ONE UEM vous permet d'importer en masse les attributs personnalisés et leurs valeurs correspondantes dans le système. Dans les modèles fournis, chaque colonne correspond à un attribut personnalisé et chaque ligne, à ses différents paramètres.

Avec les modèles, vous pouvez importer des attributs personnalisés de différentes manières et avec des informations différentes.

Attention la syntaxe de la première colonne de chaque modèle doit être répliquée exactement. L'utilisation de la syntaxe incorrecte peut créer des problèmes de base de données et des pertes de données.

Types de modèle

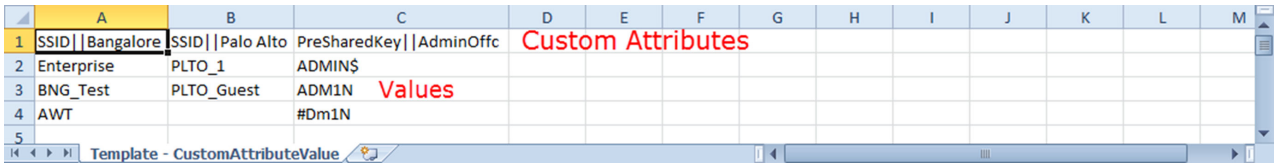
- Modèle d'attributs personnalisés – Vous permet de définir un attribut personnalisé et ses paramètres.



	A	B	C	D	E	F	G
1	CustomAttributeName	Description	ApplicationName	UsedInRuleGenerator	CollectValuesForRuleGenerator	Persist	ShowOnDevicesGrid
2	AgentVersion1	Airwatch Agent Description	Services1.exe	1	0	1	0
3	AgentVersion2	Airwatch Agent Description	Services1.exe	1	0	1	0
4	AgentVersion3	Airwatch Agent Description	Services1.exe	1	0	1	0
5	AgentVersion4	Airwatch Agent Description	Services1.exe	1	0	1	0

Template - CustomAttributes

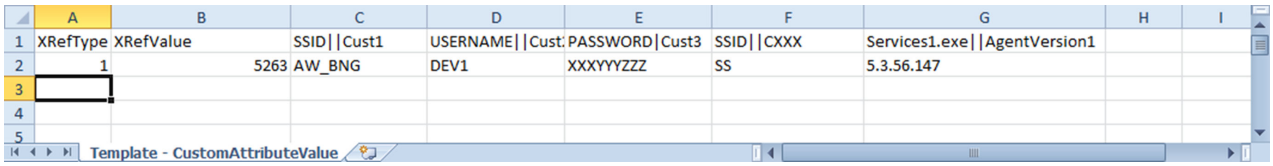
- Modèle de valeurs d'attribut personnalisées – Vous permet de définir les valeurs des attributs personnalisés prédéfinis.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	SSID||Bangalore	SSID||Palo Alto	PreSharedKey||AdminOffc	Custom Attributes									
2	Enterprise	PLTO_1	ADMIN$										
3	BNG_Test	PLTO_Guest	ADM1N	Values									
4	AWT		#Dm1N										
5													

Template - CustomAttributeValue

- Valeurs des attributs personnalisés du terminal – Vous permet de définir les valeurs des attributs personnalisés prédéfinis pour les différents terminaux basés sur la valeur de référence croisée (Xref). Les valeurs Xref déterminent les différents terminaux qui reçoivent la valeur de chaque attribut personnalisé.



	A	B	C	D	E	F	G	H	I
1	XRefType	XRefValue	SSID||Cust1	USERNAME||Cust2	PASSWORD|Cust3	SSID||CXXX	Services1.exe||AgentVersion1		
2	1	5263	AW_BNG	DEV1	XXXYYYZZZ	SS	5.3.56.147		
3									
4									
5									

Template - CustomAttributeValue

  a DeviceID (ID de terminal attribué par Workspace ONE UEM lors de l'enrôlement du terminal)

  b Numéro de série

  c UDID

  d Adresse Mac

  e Numéro IMEI

Enregistrez le fichier au format .csv avant de l'importer.

Commandes effectués sur les terminaux des élèves

6

Affichez une description détaillée de chaque action qui peut être exécutée sur un terminal, à distance, depuis la Workspace ONE UEM Console. Cette liste est indépendante de la plateforme.

Accédez à **Terminaux > Affichage en liste**, puis sélectionnez un ou plusieurs terminaux en cochant la case à gauche de chaque terminal. Appuyez ensuite sur le bouton **Plus d'actions** pour découvrir les actions que vous pouvez effectuer sur le ou les terminaux sélectionnés. Pour plus d'informations, reportez-vous à Actions en masse dans l'affichage en liste des terminaux.

- **Ajouter une balise** – Attribuez une balise personnalisable à un terminal, pour pouvoir l'identifier au sein de la flotte.
- **Applications (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir la liste des applications installées.
- **Livres (Requête)** – Envoyez une requête au terminal pour qu'il envoie une liste des livres installés.
- **Certificats (Requête)** – Envoyez une requête MDM au terminal pour recevoir une liste des certificats installés.
- **Modifier le code d'accès du terminal** – Remplacez n'importe quel code d'accès utilisé pour accéder au terminal sélectionné par un nouveau code d'accès. Le nouveau code secret s'affiche sur l'écran Modifier le code secret.
  - Notez le code secret *avant* de cliquer sur le bouton **Modifier le code secret**.
  - Cliquez sur le bouton **Modifier le code secret** pour continuer.

    - Vous pouvez fermer la fenêtre ou cliquer sur **Annuler** et revenir plus tard, ce qui signifie que si vous ne pouvez pas noter le code secret ou le transmettre à l'utilisateur final, vous pouvez relancer une action Modifier le code secret ultérieurement.
- **Modifier le groupe organisationnel** – Remplacez le groupe organisationnel d'origine du terminal par un autre groupe organisationnel existant. Comprend une option pour sélectionner un groupe organisationnel statique ou dynamique.
    - Si vous souhaitez modifier le groupe organisationnel de plusieurs terminaux à la fois, vous devez sélectionner des terminaux pour effectuer une action en masse à l'aide de la méthode de sélection de bloc (en utilisant la touche Maj) au lieu de sélectionner la case principale (en regard de l'en-tête de la colonne Dernière connexion visible dans la vue de la liste des terminaux).
- **Modifier le type de propriété** – Modifiez les paramètres de propriété d'un terminal le cas échéant. Les différents types sont : professionnel, partagé, personnel et non défini.
- **Désactiver le verrou d'activation** – Désactivez le verrou d'activation sur un terminal iOS. Si le verrou d'activation est activé, l'utilisateur doit disposer d'un identifiant Apple et d'un mot de passe avant de pouvoir utiliser les fonctions suivantes : Localiser mon iPhone, Réinitialiser le terminal avec les paramètres usine et Réactiver pour utiliser le terminal.
- **Supprimer le code d'accès (Conteneur)** – Supprimez le code d'accès spécifique du conteneur. À utiliser si l'utilisateur oublie le code d'accès au conteneur de son terminal.
- **Supprimer le code d'accès (Terminal)** – Supprimez le code d'accès du terminal. À utiliser si l'utilisateur oublie le code d'accès au conteneur de son terminal.
- **Supprimer le code secret (Paramètres de restriction)** – La commande Supprimer le code secret supprime le code secret du terminal. Le terminal doit être supervisé.
- **Supprimer le terminal** – Supprimez et annulez l'inscription d'un terminal depuis la console. Envoie la commande d'effacement des données professionnelles au terminal qui est effacé lors de l'archivage suivant et marque le terminal comme **Suppression en cours** sur la console. Si la protection contre l'effacement est désactivée sur le terminal, la commande émise effectue immédiatement un effacement des données professionnelles et supprime la représentation du terminal dans la console.
- **Informations sur le terminal (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir des informations telles que le nom convivial, la plate-forme, le modèle, le groupe organisationnel, la version du système d'exploitation et le statut de propriété.
- **Réinitialisation du terminal** – Envoyez une commande MDM pour effacer toutes les données et le système d'exploitation d'un terminal. Cette action est irréversible.
    - Considérations relatives à la réinitialisation de terminal iOS
        - Pour les terminaux iOS 11 et versions antérieures, la commande d'effacement du contenu du terminal efface également les données de la carte SIM Apple associées aux terminaux.

        - Pour les terminaux iOS 11 et versions ultérieures, vous pouvez conserver le forfait de données de la carte SIM Apple (si disponible sur les terminaux). Cochez la case **Conserver le forfait de données** sur la page Effacement du contenu du terminal avant d'envoyer la commande d'effacement du contenu du terminal.
        - Pour les terminaux iOS 11.3 et versions ultérieures, vous disposez d'une option supplémentaire pour ignorer l'écran **Configuration de la proximité** lors de l'envoi de la commande d'effacement du contenu du terminal. Lorsque l'option est activée, l'écran Configuration de la proximité est ignoré dans l'Assistant de configuration, empêchant ainsi l'utilisateur du terminal de voir l'option Configuration de la proximité.
    - Pour les terminaux Windows Desktop, vous pouvez sélectionner le type d'effacement du contenu du terminal.
        - **Effacer** : cette option efface tout le contenu du terminal.
        - **Effacement protégé** : cette option est identique à celle d'effacement normal du contenu du terminal, mais elle ne peut pas être contournée par l'utilisateur final du terminal. La commande d'effacement protégé continue d'essayer de réinitialiser le terminal jusqu'à ce qu'elle réussisse. Dans certaines configurations de terminal, cette commande peut empêcher le terminal de démarrer.
        - **Effacer et conserver les données de provisionnement** : cette option efface le contenu du terminal, mais indique que les données de provisionnement doivent être sauvegardées dans un emplacement permanent. Une fois l'effacement effectué, les données de provisionnement sont restaurées et appliquées au terminal. Le dossier de provisionnement est enregistré. Vous pouvez accéder au dossier en naviguant sur le terminal jusqu'à `%ProgramData%\Microsoft\Provisioning`.
- **Modifier le terminal** – Modifiez les informations du terminal, telles que le **nom convivial**, le **numéro d'actif**, le type de **propriété**, le type de **groupe**, la **catégorie**.
- **Activer/Désactiver le mode Perdu** – Utilisez cette fonctionnalité pour verrouiller un terminal et envoyer un message, un numéro de téléphone ou un SMS à l'écran verrouillé. L'utilisateur

final du terminal ne peut pas désactiver le mode Perdu. Lorsqu'un administrateur désactive le mode Perdu, le terminal rétablit la fonctionnalité normale. Les utilisateurs reçoivent un message qui leur indique que l'emplacement du terminal a été partagé. (iOS 9.3 + mode Supervisé)

  - **Demander la localisation du terminal** – Envoyez une requête au terminal lorsqu'il est en mode Perdu et utilisez l'onglet Localisation pour le trouver. (iOS 9.3 + mode Supervisé)

- **Enrôler** – Envoyez un message à l'utilisateur pour enrôler son terminal. Vous pouvez également utiliser un modèle de message incluant des informations d'enrôlement, telles que des instructions détaillées et des liens utiles. Cette option est uniquement disponible sur les terminaux désenrolés.
- **Réinitialisation entreprise** – Rétablissez les paramètres d'usine du terminal en conservant uniquement l'enrôlement Workspace ONE UEM.
  - **Windows Desktop uniquement :** Réinitialisation des données d'entreprise rétablit un terminal à l'état Prêt à fonctionner lorsqu'il est endommagé ou qu'il contient des applications défaillantes. Elle réinstalle le système d'exploitation Windows tout en conservant les données utilisateur, les comptes d'utilisateurs et les applications gérées. Le terminal resynchronise les paramètres d'entreprise déployés automatiquement, les stratégies et les applications après la réinitialisation tout en continuant d'être géré par Workspace ONE.
- **Effacement des données professionnelles** – Effacez les données professionnelles du terminal pour le désenrôler et supprimer toutes ses ressources professionnelles gérées, y compris les

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

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

- **Gestionnaire de fichiers** – Démarrez un gestionnaire de fichiers dans UEM console qui vous permet d'afficher à distance le contenu d'un terminal, d'ajouter des dossiers, d'effectuer des recherches et de télécharger des fichiers.
- **Rechercher un terminal** – Envoyez un message texte à l'application Workspace ONE UEM applicable et un bip sonore destiné à aider l'utilisateur à localiser un terminal égaré. Les options de bips sonores comprennent la configuration du nombre de lectures du bip et l'intervalle entre chaque lecture, en secondes.
- **Forcer la réinitialisation du mot de passe du BIOS** – Forcez le terminal à réinitialiser le mot de passe du BIOS avec le nouveau mot de passe généré automatiquement.
- **Workspace ONE Intelligent Hub (Requête)** – Envoyez une requête à Workspace ONE Intelligent Hub sur le terminal pour vérifier qu'il est installé et fonctionne normalement.
- **Mise à jour iOS** – Transférez une mise à jour du système d'exploitation vers un ou plusieurs terminaux iOS. Ceci s'applique seulement aux terminaux supervisés, enrôlés dans le DEP et fonctionnant avec iOS 9 ou versions ultérieures.
- **Emplacement** – Obtenez l'emplacement d'un terminal en l'affichant sur une carte, grâce à la fonctionnalité GPS de Workspace ONE Intelligent Hub pour macOS. Cette action nécessite l'approbation de l'utilisateur pour activer la fonctionnalité dans les préférences système de macOS.
  - Si vous souhaitez afficher l'emplacement de plusieurs terminaux à la fois, vous devez sélectionner des terminaux pour effectuer une action en masse à l'aide de la méthode de sélection de bloc (en utilisant la touche Maj) au lieu de sélectionner la case principale (en regard de l'en-tête de la colonne Dernière connexion visible dans la vue de la liste des terminaux).
- **Verrouiller le terminal** – Envoyez une commande MDM pour verrouiller un terminal sélectionné, le rendant inutilisable jusqu'à ce qu'il soit déverrouillé.
- **Verrouiller la SSO** – Empêchez l'utilisateur du terminal d'utiliser Workspace ONE UEM Container et toutes les applications correspondantes.
- **Paramètres gérés** – Activez ou désactivez l'itinérance des appels et des données, ainsi que les points d'accès personnels.
- **Gérer les étiquettes** – Affichez les étiquettes de terminal actuellement attribuées et consultez la liste des étiquettes disponibles à attribuer sur l'écran Gérer les étiquettes.

    - Si vous souhaitez gérer des étiquettes de plusieurs terminaux à la fois, vous devez sélectionner des terminaux pour effectuer une action en masse à l'aide de la méthode de sélection de bloc (en utilisant la touche Maj) au lieu de sélectionner la case principale (en regard de l'en-tête de la colonne Dernière connexion visible dans la vue de la liste des terminaux).

- **Marquer comme ne pas déranger** – Sélectionnez un terminal à ne pas déranger pour l'empêcher de recevoir des messages, des e-mails, des profils et tout autre type d'interaction entrante. Seuls les terminaux marqués comme ne pas déranger disposent de l'option **Effacer le marquage Ne pas déranger**, qui supprime les restrictions.
- **Remplacer le niveau de journalisation des tâches** – Remplacez le niveau spécifié de journalisation des tâches sur le terminal sélectionné. Cette action définit les commentaires de journalisation des tâches transférées lors du provisionnement du produit et remplace le niveau de journalisation actuel configuré dans les paramètres du Hub Android. Le

remplacement du niveau de journalisation des tâches peut être effacé en sélectionnant l'élément de menu déroulant **Rétablir les paramètres par défaut** sur l'écran d'actions. Vous pouvez également modifier le niveau de journalisation des tâches dans la catégorie Provisionnement de produit dans les paramètres du Hub Android.

- **Profils (Requête)** – Envoyez une requête MDM au terminal pour recevoir une liste des profils de terminaux installés.
- **Approvisionner maintenant** – Configurez un produit pour un terminal. Le provisionnement permet de créer une installation commandée de fichiers, d'actions, de profils et d'applications, et de les regrouper dans un seul produit qui peut être transféré vers les terminaux.
- **Envoyer une requête à tous les terminaux** – Envoyez une commande de requête au terminal pour recevoir une liste des applications (dont Workspace ONE Intelligent Hub, le cas échéant), des livres, des certificats, des informations sur le terminal, des profils et des mesures de sécurité installés.
- **Redémarrer le terminal** – Redémarrez un terminal à distance.
- **Gestionnaire de registre** – Démarrez un gestionnaire de registre dans UEM console qui vous permet d'afficher à distance le registre OS d'un terminal, d'ajouter des clés, d'effectuer des recherches et d'ajouter des propriétés.
- **Assistance à distance** – Contrôlez un terminal pris en charge à distance à l'aide de cette fonction qui offre des outils spécifiques à la plateforme vous permettant de fournir un support et un dépannage pour le terminal. Les terminaux Android nécessitent l'installation du service de contrôle à distance.
- **Gestion à distance** – Contrôlez un terminal pris en charge à distance à l'aide de cette fonction qui lance une application de la console vous permettant de fournir un support et un dépannage pour le terminal. Les terminaux Android nécessitent l'installation du service de contrôle à distance.
- **Affichage à distance** – Activez un flux actif des données sortantes du terminal vers une destination de votre choix, ce qui vous permet d'afficher ce que l'utilisateur voit lorsqu'il utilise son terminal. Les paramètres de destination comprennent l'adresse IP, le port, le port audio, le mot de passe et le temps d'analyse.
- **Renommer le terminal** – Modifiez le nom convivial du terminal dans UEM console.
- **Demande du journal du terminal** – Demandez le journal de débogage du terminal sélectionné. Vous pouvez ensuite afficher le journal en sélectionnant l'onglet **Plus** et en cliquant sur **Pièces jointes > Documents**. Vous ne pouvez pas afficher le journal dans Workspace ONE UEM Console. Le journal est fourni sous la forme d'un fichier Zip qui peut être utilisé pour le dépannage et l'assistance.

  Lorsque vous demandez un journal, vous pouvez choisir de recevoir les journaux du **Système** ou du **Hub**. **Système** fournit des journaux au niveau du système. **Hub** fournit des journaux de plusieurs agents exécutés sur le terminal.

Android uniquement : vous pouvez récupérer des journaux détaillés à partir de terminaux Android professionnels et les afficher dans la console afin de résoudre rapidement les problèmes sur le terminal.

- **Demander le check-in du terminal** – Demandez au terminal sélectionné d'effectuer son check-in dans UEM Console. Cette action met à jour le statut de la colonne **Dernière connexion**.
- **Redémarrer Workspace ONE Intelligent Hub** – Redémarrez Workspace ONE Intelligent Hub. Cette option est utilisée pendant le dépannage lorsque le processus d'enrôlement ou d'installation du sous-module est interrompu.
- **Sécurité (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir la liste des mesures de sécurité actives (gestionnaire de terminal, chiffrement, code secret, certificats, etc.).
- **Envoyer un message** – Envoyez un message à l'utilisateur du terminal sélectionné. Choisissez entre **E-mail**, **Notification Push** (via AirWatch Cloud Messaging) et **SMS**. La notification Push requiert des applications Airwatch telles que Hub, Boxer, etc. qui doivent avoir été déployées au moins une fois.
- **Démarrer AirPlay** – Diffusez du contenu audiovisuel du terminal sur une destination AirPlay en miroir. L'adresse MAC (format « xx:xx:xx:xx:xx:xx » non sensible à la casse) de la destination est requise. Un code secret peut également être spécifié si nécessaire. Le paramètre Heure de l'analyse définit le nombre de secondes (10-300) nécessaires pour rechercher la destination. Requiert macOS 10.10 ou versions ultérieures.
- **Démarrer/Arrêter AWCM** – Démarrez/Arrêtez le service de messagerie Cloud pour le terminal sélectionné. VMware AirWatch Cloud Messaging (AWCM) simplifie l'envoi de messages et de commandes de la console d'administration. Avec AWCM, les utilisateurs finaux ne sont pas obligés de se connecter à Internet ou d'utiliser des comptes grand public tels que les identifiants Google.
- **Synchroniser le terminal** – Synchronisez le terminal sélectionné avec UEM Console, en actualisant son statut de **Dernière connexion**.
- **Gestionnaire de tâches** – Exécutez le gestionnaire de tâches dans UEM console, qui vous permet d'afficher à distance les tâches actives du terminal, notamment les éléments suivants, **nom** de la tâche, **ID du processus** et **actions** applicables que vous pouvez entreprendre.
- **Afficher le mot de passe du BIOS** – Affichez le mot de passe du BIOS du terminal qui a été généré automatiquement par Workspace ONE UEM Console. Vous pouvez afficher le **Dernier mot de passe appliqué** et le **Dernier mot de passe envoyé**.
- **Consulter le manifeste** – Affichez le **manifeste du package** du terminal au format XML depuis UEM Console. Le manifeste sur les terminaux durcis Windows répertorie les métadonnées des widgets et des applications.
- **Démarrage à chaud** – Effectuez un redémarrage du système d'exploitation sans auto-test de mise sous tension (POST).

Attributions de terminaux 7

Les attributions de terminaux vous permettent de déplacer des terminaux au sein des groupes organisationnels et des noms d'utilisateurs selon la plage d'adresses IP ou l'attribut personnalisé. Il s'agit d'une alternative à l'organisation du contenu par groupes d'utilisateurs dans Workspace ONE UEM.

Au lieu que les administrateurs déplacent automatiquement les terminaux d'un groupe organisationnel à l'autre, vous pouvez donner à la console l'ordre de déplacer les terminaux automatiquement lorsqu'ils se connectent au réseau Wi-Fi que vous définissez. Vous pouvez également déplacer des terminaux en fonction des règles d'attribut personnalisés que vous définissez.

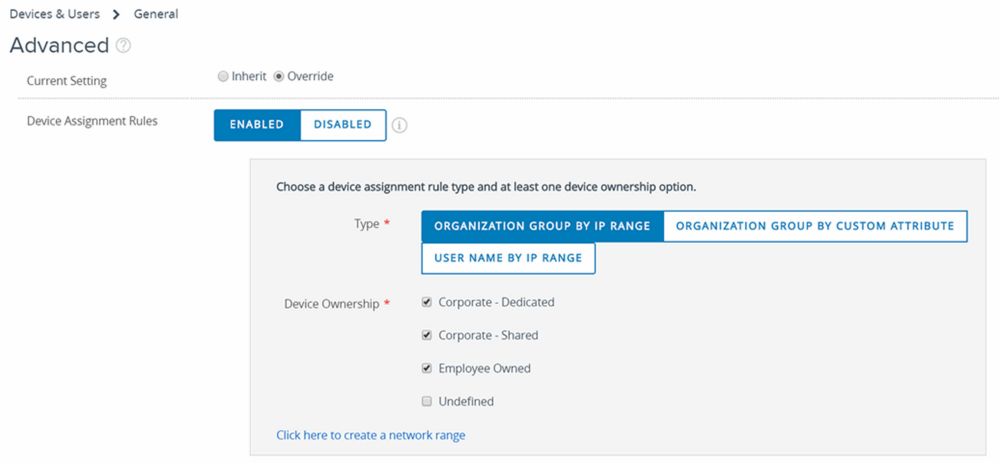
Les attributions de terminaux sont utiles dans les situations où l'utilisateur change régulièrement de rôle et requiert des profils et des applications spécialisés.

Vous devez choisir entre l'installation de **groupes d'utilisateurs** et d'**attributions de terminaux** pour déplacer les terminaux, car Workspace ONE UEM ne prend pas en charge les deux fonctions dans un même terminal.

Activer l'attribution de terminaux

Avant de pouvoir déplacer des terminaux au sein des groupes organisationnels et des noms d'utilisateurs selon l'adresse IP ou l'attribut personnalisé, vous devez activer les attributions du terminal dans Workspace ONE UEM. Les attributions de terminaux ne peuvent être configurées qu'au niveau d'un sous-groupe organisationnel.

1 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Avancé** et cliquez sur **Remplacer** ou **Hériter** le **paramètre actuel**, selon vos besoins.



2 Cliquez sur **Activé** dans le paramètre des **règles d'attributions de terminaux**.

3 Choisissez le **Type** de gestion. Les choix sont les suivants :

- **Groupe organisationnel par plage d'adresses IP** – Déplace le terminal vers un groupe organisationnel spécifié lorsqu'il quitte une plage réseau Wi-Fi et entre dans une autre. Ce déplacement déclenche le transfert automatique des profils, applications, politiques et produits.
- **Groupes organisationnels par attribut personnalisé** – Déplace le terminal vers un groupe organisationnel selon les attributs personnalisés.

  Les attributs personnalisés permettent aux administrateurs d'extraire des valeurs particulières de terminaux gérés et de les renvoyer à Workspace ONE UEM Console. Vous pouvez aussi attribuer la valeur de l'attribut aux terminaux pour le provisionnement de produit ou les valeurs de recherche.

  - Lorsque l'option **Groupe organisationnel par attribut personnalisé** est activée, un lien intitulé **Cliquer ici pour créer un attribut personnalisé en fonction de la règle d'attribution** apparaît. Lorsque ce lien est sélectionné, il ouvre un autre onglet dans votre navigateur. Cet onglet affiche la page **Règles d'attribution des attributs personnalisés** dans laquelle vous pouvez créer vos propres règles d'attribution d'attributs.
- **Nom d'utilisateur par adresse IP** – Lorsqu'un terminal quitte un réseau pour entrer dans un autre, le terminal change les noms d'utilisateur au lieu de passer à un autre groupe

organisationnel. Ce changement de nom d'utilisateur entraîne le même envoi de profils, d'applications, de politiques et de produits. Cette option est utile pour les clients ayant une capacité limitée de créer des groupes organisationnels puisqu'elle leur permet de tirer parti de la fonction d'attribution de plages réseau.

Important Si vous souhaitez modifier l'attribution **Type** dans une configuration d'attribution existante, vous devez supprimer toutes les plages définies existantes. Supprimez les attributions de plage d'adresses IP en accédant à **Groupes et paramètres > Groupes > Groupes organisationnels > Plages réseau**. Supprimez les attributions d'attributs personnalisés en accédant à **Terminaux > Provisionnement > Attributs personnalisés > Règles d'attribution d'attributs personnalisés**.

4 Sélectionnez les options de **type de propriété**. Seuls les terminaux du type de propriété sélectionné sont attribués. Les choix sont les suivants :

- Professionnel
- Professionnel, partagé
- Personnel
- Non défini

5 Vous pouvez ajouter une plage réseau en sélectionnant le lien **Cliquez ici pour créer une plage réseau**.

Vous pouvez également visiter cette page en accédant à **Groupes et paramètres > Groupes > Groupes organisationnels > Plages réseau**. La sélection des paramètres des plages réseau ne s'affiche que si les **attributions de terminaux** ont été activées pour le groupe organisationnel dans lequel vous vous trouvez lorsque vous visitez cet emplacement.

Lorsque vous cliquez sur ce lien, la page **Plages réseau** s'affiche.

6 Cliquez sur **Enregistrer** une fois toutes les options définies.

Définir la règle d'attribution ou la plage réseau

Lorsque votre terminal est connecté par Wi-Fi tout en étant géré par Workspace ONE UEM, il sera authentifié et installera automatiquement les profils, les applications, les stratégies et les provisionnements de produits spécifiques du groupe organisationnel choisi.

Vous pouvez définir des règles selon les attributs personnalisés. Lorsqu'un terminal avec un attribut personnalisé est enrôlé, la règle attribue le terminal au groupe organisationnel configuré. Le terminal peut également être attribué au cas où il reçoit une provision de produit contenant un attribut personnalisé qualifiant.

Les attributions de terminaux ne peuvent être configurées qu'au niveau d'un sous-groupe organisationnel.

1 Accédez à **Groupes et paramètres > Groupes > Groupes organisationnels > Plages réseau**.

L'option Plages réseau ne s'affiche pas tant que vous n'avez pas activé les attributions de terminaux. Ainsi, si vous ne trouvez pas « Plages réseau » dans le chemin de navigation Groupes organisationnels, reportez-vous à la section ci-dessus intitulée **Activer l'attribution de terminaux**.

2 Pour ajouter une seule plage d'adresse IP, cliquez sur **Ajouter une plage réseau**. Sur la page **Ajouter ou modifier la plage réseau**, remplissez les champs suivants puis cliquez sur **Enregistrer**.

Tableau 7-1. Ajouter une plage réseau

Paramètre	Description
Adresse IP de début	Entrez la limite supérieure de la plage réseau.
Adresse IP de fin	Entrez la limite inférieure de la plage réseau.
Nom du groupe organisationnel	Saisissez le nom du groupe organisationnel vers lequel les terminaux seront déplacés lors de la saisie de la plage réseau. Ce paramètre est uniquement visible si le **type** d'attribution réseau est défini sur « Groupe organisationnel par adresse IP ».
Nom d'utilisateur	Saisissez le nom d'utilisateur auquel les terminaux seront attribués lors de la saisie de la plage réseau. Ce paramètre est uniquement visible si le **type** d'attribution réseau est défini sur « Nom d'utilisateur par adresse IP ».
Description	Éventuellement, ajoutez une description utile de la plage réseau.

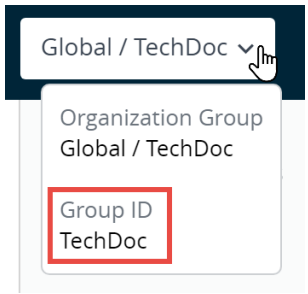
La superposition de plages réseau génère le message suivant : « Échec de l'enregistrement. La plage réseau existe. »

3 Si vous avez plusieurs plages réseau à ajouter, vous pouvez cliquer sur **Importation par lots** pour gagner du temps.

   a Sur la page d'importation par lots, sélectionnez le lien **Télécharger le modèle pour ce type de lot** pour afficher et télécharger le modèle d'importation par lots au format CSV.

b Ouvrez le fichier CSV. Le fichier CSV comporte plusieurs colonnes correspondant aux options qui s'affichent sur l'écran **Ajouter une plage réseau**. Entrez l'ID du groupe organisationnel dans la colonne « OrganisationGroup » au lieu du nom du groupe organisationnel.

Note Vous pouvez identifier l'ID de groupe d'un groupe organisationnel 1) en vous déplaçant vers le groupe organisationnel que vous souhaitez identifier et 2) en pointant votre curseur sur l'étiquette du groupe organisationnel qui affiche une fenêtre contextuelle contenant l'ID de groupe.

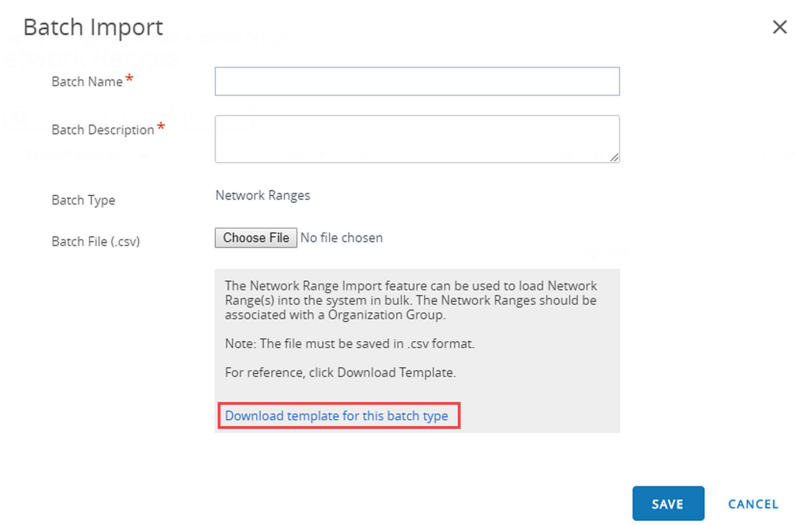


Note un fichier de valeurs séparées par des virgules (CSV, comma-separated values) est simplement un fichier texte dont l'extension a été modifiée de « TXT » en « CSV ». Il stocke les données tabulaires (chiffres et texte) en texte brut. Chaque ligne ou rangée du fichier est un enregistrement de données. Chaque enregistrement se compose d'un ou de plusieurs champs séparés par des virgules. Il peut être ouvert et modifié avec un éditeur de texte quelconque. Il peut également être ouvert et modifié avec Microsoft Excel.

c Lorsque vous ouvrez le modèle CSV, notez que des exemples de données ont été ajoutés pour chaque colonne du modèle. Les exemples de données sont présentés pour vous informer du type de données et du format requis. Ne modifiez pas le format présenté dans les exemples de données. Complétez ce modèle en remplissant chacune des colonnes requises pour chaque plage réseau que vous souhaitez ajouter.

d Importez le modèle complété à l'aide de la page **Importation par lots**.

e Cliquez sur **Enregistrer**.


Batch Import
Batch Name *
Batch Description *
Batch Type
Network Ranges
Batch File (.csv)
Choose File
No file chosen
The Network Range Import feature can be used to load Network Range(s) into the system in bulk. The Network Ranges should be associated with a Organization Group.
Note: The file must be saved in .csv format.
For reference, click Download Template.
Download template for this batch type
SAVE
CANCEL

Détails du terminal

8

Vous pouvez afficher les informations relatives à un terminal spécifique et accéder rapidement aux actions de gestion des utilisateurs et des terminaux en ouvrant la page Détails du terminal dans Workspace ONE UEM.

Vous pouvez accéder aux détails du terminal en cliquant sur le nom convivial d'un terminal depuis l'un des tableaux de bord disponibles ou en utilisant n'importe quel outil de recherche proposé dans Workspace ONE UEM Console. Un **nom convivial** est l'étiquette que vous attribuez à un terminal pour vous aider à le différencier des terminaux de la même marque et du même modèle.

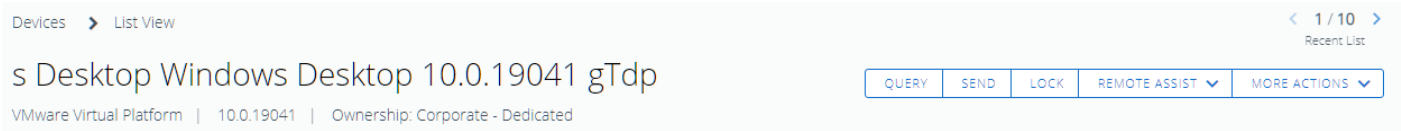
Sections importantes de la page principale

- **Badges de notification** – Affiche le statut de compromission, les violations de la conformité, la date d'enrôlement, l'heure de la dernière connexion pour le terminal sélectionné et la disponibilité du service GPS/Localisation (pour les terminaux Android uniquement).
- **Sécurité** – Affiche des paramètres de sécurité comme le logiciel de gestion utilisé pour l'enrôlement, le statut du code secret et les protections des données.
  - Si vous enrôlez un terminal avec l'application Web ou l'application Container et que vous téléchargez et exécutez ultérieurement l'application Workspace ONE Intelligent Hub sur le terminal, l'indicateur « géré par Container » devient « Hub enregistré » pour refléter la présence du Workspace ONE Intelligent Hub.
- **Informations sur l'utilisateur** – Affiche des informations basiques sur l'utilisateur, dont le nom complet et l'e-mail.
- **Informations sur le terminal** – Affiche des détails sur le terminal tels que le groupe organisationnel, la localisation, les Smart Groups, le numéro de série et d'autres étiquettes identifiantes, l'état de l'alimentation, la capacité de stockage, la mémoire physique, les détails de la garantie, la dernière heure de redémarrage (Android uniquement) et les balises de terminal par ordre alphabétique. L'intégrité de la batterie s'applique uniquement aux terminaux Android Zebra.
- **Profils** – Affiche tous les profils, qu'ils soient installés (actifs), attribués (inactifs) ou non gérés (chargé latéralement).
- **Applications** - Affiche toutes les applications installées, qu'elles soient automatiques ou à la demande.

- **Contenu** – Affiche le contenu marqué comme « Requis » par l'administrateur dans le référentiel géré par Workspace ONE UEM et dans le référentiel administrateur.
- **Certifications** – Affiche tous les certificats installés, y compris ceux qui s'apprêtent à expirer.
- **Applications administrateur** – Affiche les informations sur l'instance de Workspace ONE Intelligent Hub installée, y compris le numéro de version.
- **Informations sur la batterie Zebra** (pour les terminaux Zebra Android uniquement) – Affiche des informations détaillées sur la batterie, y compris son état, sa date de fabrication, son numéro de série et sa référence.

Tableau de bord Détails du terminal

Le tableau de bord affiche des informations de base sur le terminal, telles que le nom convivial du terminal. Il affiche également des informations détaillées, notamment le type de terminal, le modèle du terminal, le numéro de version du système d'exploitation, le type de propriété, le cluster de boutons d'actions de terminal et l'indicateur Liste récente.



La sélection des flèches dans l'indicateur d'**éléments récents** change le terminal sélectionné selon sa position dans l'**affichage en liste** filtré.

Vous pouvez également initier une session d'**Assistance à distance** sur des terminaux éligibles. Pour plus d'informations, reportez-vous à la section Assistance à distance.

Onglets du menu

Onglet du menu	Description
Résumé	Affichez les statistiques générales telles que : Applications, Mises à jour disponibles du système d'exploitation, Certificats, Contenu, Informations sur le terminal, Sécurité, Fenêtre de temps et Informations sur l'utilisateur.
Conformité	Affichez le statut, le nom de la politique, les dates de la dernière et de la prochaine vérification de conformité et les actions déjà entreprises sur le terminal. L'onglet **Conformité** comprend les fonctionnalités de résolution des problèmes : ■ Les terminaux non conformes ainsi que ceux dont le statut de conformité est en attente disposent de fonctions de résolution des problèmes. Vous pouvez réévaluer la conformité sur une base par terminal ( ) ou obtenir des informations détaillées sur l'état de conformité sur le terminal ( ). ■ Les utilisateurs avec privilèges de lecture seule peuvent voir la politique de conformité spécifique directement depuis l'onglet **Conformité** tandis que les administrateurs sont en mesure de la modifier.
Profils	Affichez tous les profils actuellement attribués, installés et non gérés sur un terminal.

Onglet du menu	Description
Applications	Affichez toutes les applications actuellement attribuées et installées sur le terminal. La colonne **Conformité des applications** identifie les applications intégrées au SDK non conformes avec les paramètres Conformité de l'application SDK. Vous trouverez ces paramètres dans **Groupes et paramètres > Tous les paramètres > Paramètres et stratégies > Conformité de l'application SDK**.
Contenu	Affichez le statut, le type, le nom, la version, la priorité, le déploiement, la dernière mise à jour, la date, l'heure de consultation et le contenu du terminal marqué comme « Requis » par l'administrateur dans le référentiel géré par Workspace ONE UEM. Cet onglet fournit également une barre d'outils pour les actions administratives (installer ou supprimer).
Emplacement	Affichez la localisation actuelle d'un terminal ou son historique de localisation. Sélectionnez la **période** ou la durée pendant laquelle vous **recherchez** les points de données d'emplacement. Le paramètre Période personnalisée vous permet de sélectionner une plage de dates et d'horaires par paliers de 5 minutes. Vous pouvez également consulter les coordonnées de latitude et de longitude de ces points de données en déplaçant le pointeur au-dessus de marqueurs d'emplacement sur la carte. Activez la collecte des données d'emplacement en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs**, puis en sélectionnant la page **Paramètres du Hub** propre à la plateforme. Pour plus d'informations sur les données de localisation en lien avec la confidentialité, consultez la rubrique Meilleures pratiques relatives à la confidentialité. Modifiez le nombre de points de données d'emplacement collectés et la distance minimum entre ces lieux en naviguant vers **Groupes et paramètres > Tous les paramètres > Installation > Cartes**.
Utilisateur	Accédez aux détails concernant l'utilisateur d'un terminal et le statut des autres terminaux enrôlés pour cet utilisateur.
Fenêtre de temps	Affichez des détails sur la fenêtre de temps attribuée au terminal, notamment son état de synchronisation, l'état appliqué, l'heure et les détails de la planification. Vous pouvez inviter les utilisateurs à sélectionner **Synchroniser le terminal** depuis l'application Workspace ONE Intelligent Hub afin de mettre à jour l'état de synchronisation. Les événements de la fenêtre de temps sont consignés par l'enregistreur des événements lorsque le niveau de journalisation minimal est défini sur **Information** ou **Débogage**. Pour plus d'informations, consultez le documentJournaux des événements.

Onglet du menu	Description
Plus	Ces onglets supplémentaires dépendent de la plateforme. ■ **Réseau** – Affichez le statut actuel du réseau (cellulaire, Wi-Fi, Bluetooth, IMEI) d'un terminal. ■ **Sécurité** – Affichez le statut de sécurité actuel d'un terminal, en fonction des paramètres de sécurité. ■ **Télécoms** – Affichez le nombre d'appels, de messages, et la quantité de données envoyés et reçus pour ce terminal. ■ **Remarques** – Visualisez et ajoutez des remarques concernant le terminal. Par exemple, indiquez son statut d'expédition ou si le terminal est en réparation ou hors service. ■ **Certificats** – Identifiez les certificats des terminaux par nom et émetteur. Cet onglet fournit aussi les dates d'expiration des certificats. ■ **Produits** – Affichez l'historique complet et le statut de tous les modules de produits provisionnés sur le terminal, ainsi que les éventuelles erreurs de déploiement. Vous pouvez également forcer le retraitement (redéploiement) d'un produit. ■ **Conditions d'utilisation** – Affichez la liste des contrats de licence utilisateur final (EULA) qui ont été acceptés lors de l'enrôlement.

Plus,continuer.	■ **Alertes** – Affichez toutes les alertes associées au terminal.
	■ **Livres** – Affichez toutes les livres internes du terminal.
	■ **Journal du terminal partagé** – Affichez l'historique du terminal partagé, notamment les dernières connexions et déconnexions et le statut.
	■ **Restrictions** – Affichez toutes les restrictions appliquées au terminal. Cet onglet affiche également des restrictions par terminal, application, note et code d'accès.
	■ **Historique du statut** – Affichez l'historique du statut d'enrôlement du terminal.
	■ **Journalisation ciblée** – Affichez les journaux de la console, du catalogue, des services de terminaux, de la gestion des terminaux et du portail en libre-service. Vous devez activer la journalisation ciblée dans les paramètres. Un lien est prévu à cet effet. Vous devez ensuite sélectionner le bouton **Créer un nouveau journal** et choisir la durée de la collecte du journal.
	■ **Dépannage** – Affichez les données de consignation **Journal des événements** et **Commandes**. Cette page propose des fonctions d'exportation et de recherche, vous permettant d'effectuer des recherches et des analyses ciblées.
	  ■ **Journal des événements** – Affichez les informations détaillées de débogage et les check-ins sur le serveur, en les **filtrant** notamment par **type de groupe d'événements**, **période**, **gravité**, **module** et **catégorie**.
	  Dans la liste **Journal des événements**, la colonne **Données de l'événement** pourrait afficher des liens hypertextes pointant vers une page contenant encore plus d'informations relatives à l'événement. Cette information vous permet d'effectuer un dépannage avancé pour, par exemple, déterminer pourquoi un profil ne peut pas être installé.
	  ■ **Commandes** – Affichez une liste détaillées des commandes terminées et en attente, envoyées au terminal. Contient un **filtre** qui vous permet de trier les commandes par **catégorie**, **statut** et **commande** spécifique.
	■ **Pièces jointes** – Utilisez cet espace de stockage sur le serveur pour les captures d'écran, les documents, les journaux d'affichage Hub envoyés par Intelligent Hub et les liens destinés au dépannage et à d'autres fins sans occuper de l'espace sur le terminal.
	■ **Détection du statut de compromission** – Affichez des informations sur le statut de compromission du terminal, y compris la **raison** spécifique du statut et son degré de **gravité**.

Enrôlement du terminal

9

L'enrôlement d'un terminal est obligatoire avant de pouvoir gérer celui-ci à l'aide de Workspace ONE UEM powered by AirWatch. Il existe plusieurs chemins d'accès à l'enrôlement, chacun incluant des options.

Raisons pour lesquelles vous ne devez pas enrôler de terminaux dans Global

Il est déconseiller d'enrôler les terminaux directement au niveau supérieur du groupe organisationnel (appelé communément Global pour plusieurs raisons. Il s'agit de la mutualisation, de l'héritage et de la fonctionnalité.

Mutualisation

Vous pouvez créer autant de groupes organisationnels enfants que nécessaire et configurer chacun d'entre eux indépendamment. Les paramètres que vous appliquez à un groupe organisationnel enfant n'ont aucun impact sur les autres groupes enfants.

Héritage

Les modifications apportées au niveau d'un groupe organisationnel parent s'appliquent aux enfants. De la même manière, les modifications apportées à un groupe organisationnel enfant ne s'appliquent pas au parent ou aux autres enfants.

Fonctionnalité

Certains paramètres et fonctionnalités ne peuvent être configurés que pour les groupes organisationnels de type Client. Cela inclut la protection contre la réinitialisation, les télécommunications et le contenu personnel. Les terminaux ajoutés directement au groupe organisationnel de niveau supérieur Global sont exclus de ces paramètres et fonctionnalités.

Le groupe organisationnel Global est conçu pour héberger le groupe Client et d'autres types de groupes organisationnels. Étant donné le fonctionnement de l'héritage, si vous ajoutez des terminaux au groupe Global et configurez ce groupe avec des paramètres ayant une incidence sur ces terminaux, vous modifiez également tous les sous-groupes organisationnels Client. Cela réduit les avantages de la mutualisation et de l'héritage.

Ce chapitre contient les rubriques suivantes :

- Enrôler un terminal auprès de Workspace ONE Intelligent Hub

- Flux de travail d'enrôlement supplémentaires
- Restrictions d'enrôlement supplémentaires
- Enrôlement par détection automatique
- Enrôlement basique vs. enrôlement par services d'annuaire
- Enrôlement BYOD (Bring Your Own Device)
- Configurer les options d'enrôlement
- Enregistrement des terminaux sur liste bloquée et liste autorisée
- Enregistrement du terminal
- État de l'enrôlement
- Auto-enrôlement ou préenrôlement
- Ordre de priorité des groupes organisationnels pour l'enrôlement des utilisateurs
- Enrôlement direct de Workspace ONE

Enrôler un terminal auprès de Workspace ONE Intelligent Hub

L'enrôlement d'un terminal auprès de Workspace ONE Intelligent Hub est la principale option pour les terminaux Android, iOS et Windows dans Workspace ONE Express et Workspace ONE UEM powered by AirWatch.

Procédure

1 Téléchargez et installez Workspace ONE Intelligent Hub depuis Google Play Store (pour les terminaux Android) ou depuis l'App Store (pour les terminaux Apple).

Le téléchargement de Workspace ONE Intelligent Hub depuis une boutique d'applications publiques nécessite un ID Apple ou un compte Google.

Les terminaux **Windows 10** doivent diriger le navigateur par défaut du terminal sur https://getwsone.com pour télécharger le Hub.

2 Exécutez Workspace ONE Intelligent Hub à l'issue du téléchargement ou revenez à votre session de navigateur.

Important Pour une installation et un fonctionnement sans problème de Workspace ONE Intelligent Hub sur un terminal Android, le terminal doit disposer de 60 Mo d'espace libre minimum. Sur la plateforme Android, le processeur et la mémoire d'exécution sont alloués par application. Si une application utilise plus de ressources que celles qui lui sont allouées, les terminaux Android l'arrêtent afin d'optimiser leurs performances.

3 Saisissez votre adresse e-mail lorsque vous y êtes invité. Workspace ONE UEM Console vérifie si votre adresse a déjà été ajoutée à l'environnement. Si c'est le cas, vous êtes déjà configuré en tant qu'utilisateur final et votre groupe organisationnel vous a déjà été attribué.

   Si Workspace ONE Console ne peut pas vous identifier en tant qu'utilisateur final d'après votre adresse e-mail, vous serez invité à indiquer votre **Serveur**, votre **ID de groupe** et vos **identifiants**. Si votre URL d'environnement et votre ID de groupe sont nécessaires, votre administrateur Workspace ONE peut vous les fournir.

4 Finalisez l'enrôlement en suivant tous les autres messages qui s'affichent. Vous pouvez utiliser votre adresse e-mail à la place du nom d'utilisateur. Si deux utilisateurs ont la même adresse e-mail, l'enrôlement échoue.

Résultats

Le terminal est maintenant enrôlé sur l'application Workspace ONE Intelligent Hub. Dans l'onglet **Résumé** de la **Vue détaille du terminal** pour ce terminal, le panneau de sécurité affiche « Hub enregistré » pour refléter cette méthode d'enrôlement.

Pour plus d'informations, reportez-vous à Chapitre 8 Détails du terminal.

Flux de travail d'enrôlement supplémentaires

Dans certains cas, le processus d'enrôlement dans Workspace ONE UEM powered by AirWatch doit être adapté à des organisations ou des déploiements spécifiques. Pour chacune des options d'enrôlement supplémentaires, les utilisateurs finaux doivent utiliser les identifiants fournis dans la section Informations requises de ce guide.

- **Environnements multi-domaines** – Les identifiants de connexion pour l'enrôlement dans les environnements à un seul domaine et multi-domaines sont pris en charge s'ils sont fournis au format suivant. **domaine\nom d'utilisateur**.
- **Mode Kiosque et concepteur de kiosques** – Les utilisateurs finaux de postes de travail Windows peuvent configurer leurs terminaux en mode Kiosque. Les utilisateurs peuvent également utiliser le concepteur de kiosques dans la console Workspace ONE UEM pour créer un kiosque multi-applications.
- **Enrôlement par invitation** – L'utilisateur final reçoit une notification (par e-mail ou SMS) contenant l'URL d'enrôlement et saisit son ID de groupe ainsi que ses identifiants de connexion. Lorsque l'utilisateur final accepte les conditions d'utilisation, le terminal est automatiquement enrôlé et équipé de toutes les fonctionnalités et de l'ensemble du contenu MDM. Cette acceptation comprend des applications et fonctionnalités sélectionnées depuis le serveur Workspace ONE UEM.

- **Enrôlement en un clic** – Dans ce processus qui s'applique aux enrôlements basés sur le Web, l'administrateur envoie à l'utilisateur un jeton généré par Workspace ONE UEM ainsi qu'une URL d'enrôlement. L'utilisateur n'a qu'à sélectionner le lien fourni pour s'authentifier et enrôler le terminal, ce qui facilite et accélère grandement le processus d'enrôlement pour l'utilisateur. Cette méthode peut également être sécurisée par un paramètre d'expiration dans le temps.
  - **Enrôlement par le Web** – L'administrateur peut faire appel à un écran d'accueil facultatif pour les enrôlements Web en ajoutant « /enroll/welcome » à l'environnement actif. Par exemple, si vous fournissez l'URL **https://<environnementperso > /enroll/welcome** aux utilisateurs participant à l'enrôlement par le Web, ils verront apparaître un écran Bienvenue dans Workspace ONE UEM. Cet écran comprend des options pour s'enrôler avec une adresse e-mail ou un ID de groupe. L'option d'enrôlement par le Web s'applique à Workspace ONE UEM versions 8.0 et supérieures.
- **Double authentification** – Dans ce processus, l'administrateur envoie le même jeton d'enrôlement généré par Workspace ONE UEM, mais l'utilisateur doit également saisir ses identifiants de connexion. Cette méthode est tout aussi facile à exécuter que l'enrôlement en un clic, mais fournit un niveau de sécurité supplémentaire. La mesure de sécurité supplémentaire consiste à demander à l'utilisateur de saisir ses identifiants personnels.
- **Inscription par l'utilisateur final** – L'utilisateur se connecte au portail en libre-service et inscrit son propre terminal. Une fois l'inscription terminée, le système envoie à l'utilisateur final un e-mail contenant l'URL d'enrôlement et les identifiants de connexion. Ce processus présuppose que les administrateurs n'ont pas encore effectué d'inscription de terminaux pour la flotte de terminaux professionnels. Il suppose également que vous requérez que les terminaux professionnels soient inscrits pour que les administrateurs puissent consulter le statut d'enrôlement. En outre, l'enregistrement de l'utilisateur final signifie que les terminaux professionnels peuvent être utilisés avec des terminaux achetés par l'utilisateur.
- **Préenrôlement de terminaux à utilisateur unique** – L'administrateur enrôle les terminaux pour un utilisateur. 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. L'administrateur peut aussi configurer et enrôler un terminal et l'envoyer directement à un utilisateur qui n'est pas sur place.
- **Préenrôlement de terminaux partagés** – L'administrateur enrôle des terminaux qui seront utilisés par plusieurs personnes. Chaque terminal est enrôlé et équipé d'un ensemble de fonctionnalités spécifiques auxquelles les utilisateurs ont accès uniquement après s'être connectés avec leurs identifiants personnels.

Restrictions d'enrôlement supplémentaires

Vous pouvez définir des restrictions d'enrôlement supplémentaires afin de contrôler qui procède à l'enrôlement dans Workspace ONE UEM et quels types de terminaux sont autorisés.

La mise en place de restrictions d'enrôlement supplémentaires s'applique à tous les types de déploiement, quels que soient l'intégration des services d'annuaire, la prise en charge du BYOD, l'inscription des terminaux, ou d'autres configurations.

Vous pouvez également déterminer le nombre maximum de terminaux enrôlés par groupe organisationnel. Après avoir configuré les restrictions d'enrôlement, vous pouvez même les enregistrer en tant que politique.

Considération 1 : pensez-vous définir des limites relatives à des plateformes spécifiques, aux versions d'OS ou au nombre maximum de terminaux autorisés ?

- Voulez-vous uniquement prendre en charge les terminaux disposant de la fonction intégrée de gestion d'entreprise, tels que les appareils Samsung SAFE/Knox, HTC Sense, LG Enterprise et Motorola ? Si oui, vous pouvez demander à ce que les terminaux Android possèdent une version entreprise supportée en guise de restriction d'enrôlement.
- Voulez-vous limiter le nombre de terminaux qu'un utilisateur est autorisé à enrôler ? Si oui, vous pouvez définir ce nombre, en précisant la quantité de terminaux professionnels et de terminaux personnels.
- Certaines plateformes ne sont-elles pas prises en charge par votre déploiement ? Si oui, vous pouvez créer une liste de plateformes bloquées.

Votre organisation doit évaluer le nombre et les types de terminaux appartenant à vos employés. Elle doit également déterminer ceux qu'elle souhaite utiliser dans votre environnement de travail. Une fois que ce travail est terminé, vous pouvez enregistrer ces restrictions d'enrôlement en tant que politique.

Considération 2 : pensez-vous limiter l'enrôlement à une liste définie de terminaux professionnels ?

Les options supplémentaires d'inscription permettent de contrôler les terminaux autorisés à être enrôlés. Pour les déploiements BYOD, vous pouvez empêcher l'enrôlement des terminaux sur liste bloquée ou le limiter aux terminaux sur liste autorisée. Vous pouvez afficher les terminaux sur liste autorisée par type, plateforme, ID de terminal et numéro de série. Pour plus d'informations, reportez-vous à Enregistrement des terminaux sur liste bloquée et liste autorisée.

Considération 3 : pensez-vous limiter le nombre de terminaux enrôlés par groupe organisationnel ?

Vous pouvez appliquer une limite de terminaux enrôlés pour un groupe organisationnel. Cela vous permet de gérer votre déploiement en vous empêchant de dépasser le nombre d'enrôlements valides. Pour plus d'informations, consultez la section **Limiter le nombre de terminaux enrôlés par groupe organisationnel** sur cette page.

Configurer les paramètres de restriction d'enrôlement

Lors de l'intégration de Workspace ONE UEM aux services d'annuaire, vous pouvez déterminer quels utilisateurs peuvent enrôler des terminaux dans votre déploiement professionnel.

Vous pouvez limiter l'enrôlement aux groupes configurés ou aux utilisateurs connus. Les utilisateurs connus sont ceux qui existent dans UEM Console. Les groupes configurés renvoient aux utilisateurs associés aux groupes du service d'annuaire si vous souhaitez une intégration aux groupes d'utilisateurs. Vous pouvez aussi limiter le nombre de terminaux enrôlés par groupe organisationnel et enregistrer les restrictions comme politique réutilisable.

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**. L'onglet Restrictions vous permet de personnaliser les politiques de restriction de l'enrôlement selon les rôles du groupe organisationnel ou du groupe d'utilisateurs.

- Créez et attribuez les politiques de restriction de l'enrôlement existantes à l'aide des paramètres de politique.
- Attribuez la politique à un groupe d'utilisateurs dans la section Paramètres d'attribution de groupe.
- Créez des listes bloquées ou autorisées de terminaux selon la plateforme, le système d'exploitation, l'UDID, le numéro IMEI, etc.

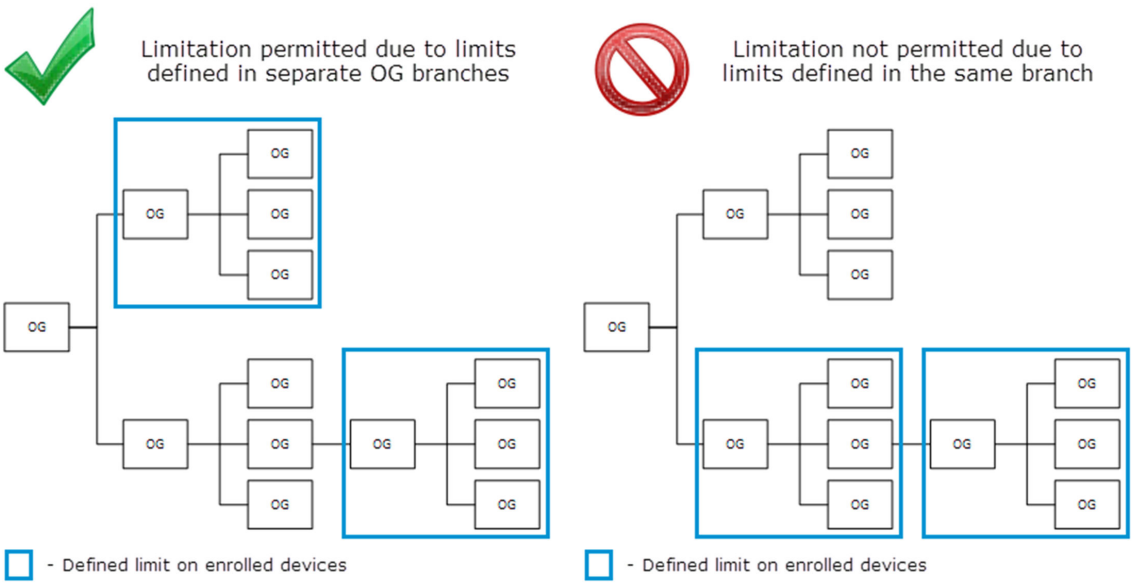
Paramètre	Description
Gestion de l'accès utilisateur	L'enrôlement direct de Workspace ONE prend en charge toutes les options de contrôle de l'accès utilisateur. **Restreindre l'enrôlement aux utilisateurs connus** – Permet de restreindre l'enrôlement aux seuls utilisateurs qui existent dans UEM Console. Cette restriction s'applique aux utilisateurs de l'annuaire que vous avez ajoutés un par un à UEM Console, manuellement ou par lot. Elle peut également être utilisée pour verrouiller un enrôlement suite à un déploiement initial autorisant tout le monde à s'enrôler. Cette option vous permet de sélectionner les utilisateurs capables de s'enrôler. Vous pouvez autoriser tous les utilisateurs de l'annuaire qui ne possèdent pas de compte dans UEM Console à s'enrôler dans Workspace ONE UEM en désactivant cette option. Les comptes utilisateur sont automatiquement créés au cours de l'enrôlement. **Restreindre l'enrôlement aux groupes configurés** –Activez cette option pour limiter l'enrôlement aux utilisateurs appartenant à tous les groupes ou aux groupes sélectionnés (en cas d'intégration aux groupes d'utilisateurs). Ne sélectionnez pas cette option si vous n'avez pas procédé à l'intégration aux groupes d'utilisateurs du service d'annuaire. **Note** La restriction de l'enrôlement aux groupes configurés est uniquement prise en charge avec l'enrôlement utilisateur Juste-à-temps (JIT), lorsque chacun des éléments suivants est vérifié : ■ Workspace ONE UEM est configuré comme la source d'authentification pour Workspace ONE Intelligent Hub, que vous configurez en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement**, puis en sélectionnant l'onglet **Authentification**. ■ SAML pour l'authentification est désactivé pour les utilisateurs d'enrôlement. Configurez ce paramètre en accédant à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > Services d'annuaire** et consultez la documentation relative aux paramètres système des services d'annuaire. Vous pouvez créer des comptes utilisateur Workspace ONE UEM lors de l'enrôlement en désactivant l'option pour autoriser tous les utilisateurs de l'annuaire à s'enrôler. Sélectionnez **Effacer les données professionnelles sur les terminaux des utilisateurs qui sont supprimés des groupes configurés** pour effacer automatiquement les données professionnelles des terminaux. Si l'option **Tous les groupes** est sélectionnée, les terminaux n'appartenant à aucun groupe d'utilisateurs sont supprimés. Si l'option **Groupes sélectionnés** est définie, les terminaux n'appartenant à un groupe d'utilisateurs spécifique sont supprimés. Une possibilité d'intégration aux groupes d'utilisateurs consiste à créer un groupe de service d'annuaire « Approuvé par le MDM », à l'importer vers Workspace ONE UEM, puis à ajouter les groupes d'utilisateurs du service d'annuaire existants au groupe « Approuvé par le MDM » lorsqu'ils sont éligibles pour Workspace ONE UEM.
Définir la limite du nombre maximum de terminaux enrôlés au niveau de ce groupe organisationnel et au niveau inférieur	Activez ce paramètre et **saisissez le nombre limite** de terminaux pour restreindre le nombre de terminaux autorisés à s'enrôler dans le groupe organisationnel actuel. L'enrôlement direct de Workspace ONE prend en charge cette option.

Note les restrictions d'enrôlement ne s'appliquent pas aux terminaux iOS enrôlés via le programme d'inscription de terminaux d'Apple (DEP), les informations requises du terminal étant seulement reçues après l'enrôlement.

Limiter le nombre de terminaux enrôlés par groupe organisationnel

Vous pouvez appliquer une limite de terminaux enrôlés pour un groupe organisationnel. Cela vous permet de gérer votre déploiement en vous empêchant de dépasser le nombre d'enrôlements valides dans un environnement d'allocation de licence par terminal.

Cette limite peut s'appliquer à tous les types de groupe organisationnel (global, client, partenaire). Lorsqu'une limite est définie sur un groupe organisationnel, vous ne pouvez pas définir d'autre limite dans la même branche de groupe organisationnel. Vous pouvez définir une limite de terminal enrôlé si vous la configurez dans une autre branche de groupe organisationnel.



Si cette option n'est pas disponible, vérifiez le groupe organisationnel parent (supérieur au groupe actuel) ou un sous-groupe (inférieur au groupe actuel). Une limite a probablement déjà été définie au-dessus ou en dessous du groupe organisationnel actuel.

1 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et sélectionnez l'onglet **Restriction**.

2 Activez la limite dans **Définir la limite du nombre maximum de terminaux enrôlés au niveau de ce groupe organisationnel et au niveau inférieur**.

Créer une politique de restriction d'enrôlement

Votre organisation doit évaluer le nombre et les types de terminaux appartenant à vos employés. Elle doit également déterminer les terminaux à utiliser dans votre environnement de travail. Une fois que ce travail est terminé, vous pouvez enregistrer ces restrictions d'enrôlement en tant que politique.

1 Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement**.

2 Sélectionnez l'onglet **Restrictions**, puis cliquez sur **Ajouter une politique**, dans la section **Paramètres de la politique**.

3 Sur la page **Ajouter/Modifier la politique de restriction d'enrôlement**, ajoutez une politique de restriction d'enrôlement.

Paramètre	Description
Nom de la politique de restriction d'enrôlement	Saisissez un nom pour votre politique de restriction d'enrôlement.
Groupe organisationnel	Sélectionnez un groupe organisationnel dans la liste déroulante. Il s'agit du groupe organisationnel auquel votre nouvelle politique de restriction d'enrôlement s'appliquera.
Type de politique	Sélectionnez le type de politique, qui peut être **Par défaut pour le groupe organisationnel** pour l'appliquer au groupe organisationnel choisi, ou **Politique des groupes d'utilisateurs** pour l'appliquer à des groupes d'utilisateurs spécifiques grâce aux paramètres d'attribution du groupe dans l'onglet **Restrictions**.
Types de propriété autorisés	Sélectionnez si vous autorisez ou non les terminaux **professionnels**, **partagés** et/ou **personnels**. L'enrôlement direct de Workspace ONE prend uniquement en charge les types de propriété professionnel et personnel.
Types d'enrôlement autorisés	Sélectionnez si vous autorisez ou non l'enrôlement des terminaux utilisant les applications **MDM** (Workspace ONE Intelligent Hub) et AirWatch **Container** (pour iOS/Android).
Nombre maximal de terminaux par utilisateur	Choisissez **Illimité** pour permettre aux utilisateurs d'enrôler autant de terminaux qu'ils le souhaitent. L'enrôlement direct de Workspace ONE prend en charge la définition d'une limite de terminaux par utilisateur. Décochez cette case pour saisir des valeurs dans la section **Nombre maximal de terminaux par utilisateur** afin de définir le nombre maximal de terminaux par type de propriété. ■ **Nombre maximum de terminaux par utilisateur** ■ **Nombre maximum de terminaux professionnels** ■ **Nombre maximum de terminaux partagés** ■ **Nombre maximum de terminaux personnels**

Paramètre	Description
Types de terminaux autorisés	Cochez la case **Limiter l'enrôlement à des plateformes, modèles ou systèmes d'exploitation spécifiques** pour ajouter des restrictions supplémentaires, propres au terminal. Cette option est prise en charge par l'enrôlement direct de Workspace ONE.
Mode de restrictions au niveau du terminal	Cette option est disponible seulement si **Limiter l'enrôlement à des plateformes, modèles ou systèmes d'exploitation spécifiques** est sélectionné dans **Types de terminaux autorisés**. Déterminez le type de limitations de terminal que vous souhaitez. ■ **Autoriser uniquement les types de terminaux répertoriés (liste autorisée)** : sélectionnez cette option pour autoriser explicitement les terminaux correspondant aux paramètres saisis et bloquer tous les autres. ■ **Bloquer les types de terminaux répertoriés (liste bloquée)** : sélectionnez cette option pour bloquer les terminaux correspondant aux paramètres saisis et autoriser tous les autres. Pour l'un ou l'autre des modes de restrictions au niveau du terminal, cliquez sur **Ajouter une restriction de terminal** afin de sélectionner une **plateforme**, un **modèle**, un **fabricant** (terminaux Android uniquement), un **système d'exploitation**. Vous pouvez aussi ajouter une **limite de terminaux** par restriction de terminal définie. Vous pouvez ajouter plusieurs restrictions de terminaux. Vous pouvez également bloquer des terminaux spécifiques en fonction de leur IMEI, numéro de série ou UDID en accédant à **Terminaux > Cycle de vie > État de l'enrôlement** et en cliquant sur **Ajouter**. Ceci est une manière efficace de bloquer un seul et unique terminal et de l'empêcher de se réenrôler sans affecter d'autres terminaux d'utilisateurs. Vous pouvez aussi empêcher le réenrôlement lors d'un effacement des données professionnelles. Cette option est prise en charge par l'enrôlement direct de Workspace ONE.

4 Cliquez sur **Enregistrer** pour sauvegarder vos modifications et revenez à l'écran **Terminaux et utilisateurs / Général / Enrôlement**.

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 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.

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.

Que faire ensuite ? 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 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.

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**.

Enrôlement basique vs. enrôlement par services d'annuaire

Vous pouvez enrôler des utilisateurs et des groupes de services d'annuaire existants comme Active Directory (AD), Lotus Domino et Novell e-Directory. Si vous ne disposez pas d'une telle infrastructure ou si vous avez choisi de ne pas l'intégrer, vous devez procéder à un enrôlement basique dans Workspace ONE UEM.

L'enrôlement basique renvoie au processus de création manuelle des comptes utilisateur et des groupes d'utilisateurs pour chacun des utilisateurs de votre organisation. Si votre organisation n'intègre pas Workspace ONE UEM avec un service d'annuaire, l'enrôlement basique correspond à la façon dont vous créez les comptes utilisateur.

Si vous devez créer un petit nombre de comptes basiques, créez-les un par un tel que décrit dans la section Créer des comptes utilisateur basiques.

Pour les enrôlements basiques impliquant un plus grand nombre d'utilisateurs finaux, vous pouvez gagner du temps en remplissant et en important des modèles CSV (valeurs séparées par des virgules). Ces fichiers contiennent toutes les informations utilisateur que vous ajoutez et sont intégrés dans UEM via la fonctionnalité d'importation par lot. Pour plus d'informations, reportez-vous à la section Importer par lots les utilisateurs ou les terminaux.

Note Alors que Workspace ONE UEM prend en charge un mélange d'utilisateurs d'enrôlement basiques et par services d'annuaire, vous utilisez l'une des deux méthodes pour l'enrôlement initial des utilisateurs et des terminaux.

Avantages et inconvénients

	Avantages	Inconvénients
Enrôlement basique	■ Peut être utilisé pour n'importe quelle méthode de déploiement. ■ Ne nécessite aucune intégration technique. ■ Ne nécessite aucune infrastructure d'entreprise. ■ Peuvent être enrôlés dans potentiellement plusieurs groupes d'organisation.	■ Les identifiants existent uniquement dans Workspace ONE UEM et ne correspondent pas nécessairement aux identifiants professionnels existants. ■ Ne propose pas de sécurité fédérée. ■ L'authentification unique n'est pas prise en charge. ■ Workspace ONE UEM stocke tous les noms d'utilisateur et mots de passe. ■ Ne peut pas être utilisé pour l'enrôlement direct de Workspace ONE.
Enrôlement du service d'annuaire	■ Les utilisateurs finaux s'authentifient grâce à leurs identifiants professionnels existants. ■ Détecte et synchronise les modifications à partir du système d'annuaire dans Workspace ONE UEM automatiquement. Par exemple, lorsque vous désactivez des utilisateurs dans AD, le compte utilisateur correspondant dans Workspace ONE UEM Console est marqué comme étant inactif. ■ Méthode sécurisée d'intégration de votre service d'annuaire existant. ■ Pratique d'intégration standard. ■ Peut être utilisé pour l'enrôlement direct de Workspace ONE. ■ Pour les déploiements SaaS utilisant AirWatch Cloud Connector, aucune modification de pare-feu n'est autorisée et la configuration sécurisée d'autres infrastructures telles que les serveurs Microsoft ADCS, SCEP, et SMTP est assurée.	■ Une infrastructure de services d'annuaire existants est obligatoire. ■ Les déploiements SaaS nécessitent une configuration supplémentaire en raison de l'installation d'AirWatch Cloud Connector derrière le pare-feu ou dans une DMZ.

Critères à prendre en compte pour l'enrôlement basique ou d'annuaire

Lorsque vous envisagez l'enrôlement de l'utilisateur final, vous devez envisager d'autres points en plus des avantages et inconvénients existants des utilisateurs à enrôlement basique et par services d'annuaire.

Considération 1 : qui peut enrôler ?

Pour répondre à cette question, prenez en compte les éléments suivants.

- Votre déploiement MDM a-t-il pour but de gérer les terminaux pour tous les utilisateurs de votre organisation au niveau du nom unique de base configuré ou au niveau inférieur ? Si c'est le cas, la meilleure façon de procéder est d'autoriser tous vos utilisateurs à s'enrôler en vous assurant que les cases Limiter l'enrôlement sont désélectionnées.

  Vous pouvez autoriser tous les utilisateurs à s'enrôler pendant le déploiement initial et limiter ensuite l'enrôlement afin d'empêcher les utilisateurs inconnus de s'enrôler. Au fur et à mesure que votre organisation ajoute de nouveaux employés ou membres aux groupes d'utilisateurs existants, ces modifications seront synchronisées et fusionnées.

- Y a-t-il des utilisateurs ou des groupes qui ne doivent pas être inclus dans MDM ? Si oui, vous devez ajouter les utilisateurs un par un ou importer par lot un fichier CSV (valeurs séparées par des virgules) d'utilisateurs autorisés uniquement.

* Le nom unique de base, ou le nom unique, est le point à partir duquel un serveur recherche des utilisateurs. Un nom unique identifie de façon unique une entrée dans le répertoire. Chaque entrée dans le répertoire dispose d'un nom unique.

Considération 2 : où les utilisateurs seront-ils attribués ?

La méthode d’attribution des utilisateurs d'annuaire aux groupes organisationnels pendant l'enrôlement est un autre élément à prendre en considération lors de l'intégration de votre environnement Workspace ONE UEM aux services d'annuaire. Pour répondre à cette question, prenez en compte les éléments suivants.

- Avez-vous créé une structure de groupes organisationnels correspondant aux groupes de vos services d'annuaire ? Vous devez effectuer cette tâche avant de pouvoir modifier l'attribution des utilisateurs.
- Si vos utilisateurs enrôlent leurs propres terminaux, il est facile de sélectionner un ID de groupe dans une liste. Cette simplicité est cependant compensée par la possibilité d'une erreur humaine, qui peut conduire à des attributions de groupe incorrectes.

Vous pouvez sélectionner automatiquement un ID de groupe en fonction d'un groupe d'utilisateurs ou autoriser les utilisateurs à choisir un ID de groupe dans une liste. Ces options de **mode d'attribution de l'ID de groupe** sont disponibles en accédant à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement** et en sélectionnant l'onglet **Regroupement**.

Activation de l'enrôlement basé sur les services d'annuaire

L'enrôlement basé sur les services d'annuaire fait référence au processus d'intégration de Workspace ONE UEM dans l'infrastructure des services d'annuaire de votre organisation. Une telle intégration de votre service d'annuaire signifie que vous pouvez importer des utilisateurs automatiquement et, éventuellement, des groupes d'utilisateurs tels que des groupes de sécurité et des listes de distribution.

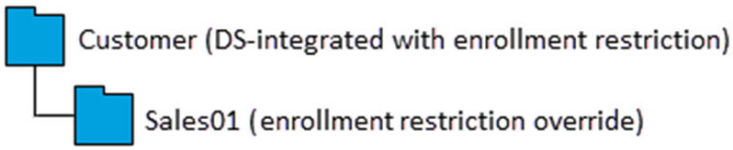
Lors de l'intégration à un service d'annuaire comme Active Directory (AD), vous avez le choix dans la manière d'importer les utilisateurs.

- **Autoriser tous les utilisateurs d'annuaire à s'enrôler** – Vous pouvez autoriser tous vos utilisateurs de service d'annuaire à s'enrôler. Vous pouvez également configurer votre environnement pour qu'il détecte automatiquement les utilisateurs en fonction de leur adresse e-mail. Créez ensuite un compte utilisateur Workspace ONE UEM pour ces utilisateurs lorsqu'ils effectuent l'enrôlement.
- **Ajouter les utilisateurs un par un** – Après l'intégration d'un service d'annuaire, vous pouvez ajouter des utilisateur un par un, comme vous le feriez pour créer des comptes utilisateur Workspace ONE UEM basiques. La seule différence est que vous devez saisir leur nom d'utilisateur et cliquer sur **Vérifier l'utilisateur** pour emplir automatiquement les informations restantes.
- **Importer par lots un fichier CSV** – Grâce à cette option, vous pouvez importer une liste de comptes de service d'annuaire dans un fichier de modèle CSV (valeurs séparées par des virgules). Ce fichier dispose de colonnes très spécifiques, certaines d'entre elles ne pouvant pas être vides.
- **Intégrer des groupes d'utilisateurs (facultatif)** – Cette méthode vous permet d'utiliser les appartenances de vos groupes d'utilisateurs existants pour attribuer des profils, des applications, des politiques de conformité, etc.

Note Pour plus d'informations sur l'intégration de votre environnement Workspace ONE UEM à votre service d'annuaire, y compris l'intégration du fournisseur SAML, reportez-vous au document Integrate Directory Service Guide.

Intégration des services d'annuaire et restrictions d'enrôlement

Lorsque l'intégration des services d'annuaire est configurée sur Workspace ONE UEM, les comptes de services d'annuaire héritent des paramètres d'enrôlement du groupe organisationnel à partir duquel le service d'annuaire est configuré. Les comptes basiques respectent néanmoins les paramètres locaux, y compris les remplacements.



En prenant le modèle de groupe organisationnel ci-dessus comme exemple, supposons que l'option **Effacer les données d'entreprise sur les terminaux des utilisateurs n'appartenant pas à des groupes configurés** est activée sur l'OG nommé Client.

Dans ce scénario, les utilisateurs inscrits dans l'**annuaire** de l'OG enfant Sales01 qui quittent un groupe configuré voient leurs terminaux effacés malgré le remplacement de la restriction d'inscription configuré dans l'OG. Ce principe s'applique même si ces comptes comportent des terminaux enrôlés sur un autre groupe organisationnel, parce que les paramètres d'enrôlement sont propres à l'utilisateur et non au terminal.

Toutefois, dans ce même scénario, les terminaux appartenant à des utilisateurs de l'enrôlement **basique** du groupe organisationnel Sales01 qui quittent un groupe configuré ne sont pas effacés. En effet, les utilisateurs d'inscription basique du Sales01 ne font pas partie de l'OG de l'annuaire intégré. Ainsi, ils reconnaissent et acceptent que les restrictions d'inscription soient remplacés.

Enrôlement BYOD (Bring Your Own Device)

L'un des principaux défis de la gestion des terminaux personnels dans Workspace ONE UEM est d'identifier et de distinguer les terminaux professionnels des terminaux personnels, puis de limiter l'enrôlement uniquement aux terminaux approuvés.

Workspace ONE UEM vous permet de configurer de nombreuses options qui permettent de personnaliser l'expérience utilisateur d'enrôlement d'un terminal personnel. Avant de commencer, vous devez déterminer comment planifier l'identification des terminaux personnels dans votre déploiement et si vous souhaitez leur appliquer des restrictions d'enrôlement.

Éléments à prendre en compte pour l'enrôlement

Si vous autorisez les employés à enrôler leurs terminaux personnels dans votre environnement Workspace ONE UEM, vous devez prendre en compte de nombreux critères au préalable.

Considération 1 : les utilisateurs BYOD s'enrôleront-ils auprès de VMware Workspace One ou de Workspace ONE Intelligent Hub ?

VMware Workspace ONE est une plateforme d'entreprise simple et sécurisée qui distribue et gère n'importe quelle application sur n'importe quel terminal. Pour commencer, elle comprend une authentification unique en libre-service pour accéder aux applications Cloud, mobiles et Windows ainsi que des outils de collaboration, de fichier, de calendrier et de messagerie solidement intégrés.

Grâce à Workspace ONE, les utilisateurs n'ont plus besoin d'enrôler leurs terminaux personnels pour accéder aux services. L'application Workspace ONE peut être téléchargée depuis l'Apple App Store, Google Play ou le Microsoft Store, avant d'être installée. Un utilisateur se connecte alors et accède aux applications en fonction des politiques établies. Workspace ONE configure un profil de gestion MDM lors de son installation ce qui permet d'enrôler automatiquement le terminal.

Considération 2 : appliquerez-vous des restrictions d'enrôlement supplémentaires pour les terminaux personnels ?

Pour répondre à cette question, prenez en compte les éléments suivants.

- Votre déploiement MDM ne prend-il en charge que certaines plateformes ? Si c'est le cas, vous pouvez préciser lesquelles et n'autoriser que l'enrôlement des terminaux fonctionnant sur ces plateformes.
- Limitez-vous le nombre de terminaux personnels qu'un employé peut enrôler ? Si c'est le cas, vous pouvez préciser le nombre maximum de terminaux qu'un utilisateur est autorisé à enrôler.

Vous pouvez définir des restrictions d'enrôlement supplémentaires afin de contrôler qui procède à l'enrôlement et quels types de terminaux sont autorisés. Vous pouvez par exemple choisir de prendre en charge uniquement les terminaux Android disposant de la fonctionnalité intégrée de gestion d'entreprise. Une fois que votre entreprise a évalué le type de terminaux que les employés possèdent et décidé lesquels d'entre eux ils souhaitent utiliser dans votre environnement professionnel, vous pouvez configurer ces paramètres.

Identifier les terminaux professionnels et préciser le type de propriété par défaut

Il est utile de préparer une liste de terminaux si vous avez un mélange de terminaux professionnels et de terminaux personnels que les employés enrôlent eux-mêmes. Lorsque l'enrôlement commence, les terminaux que vous avez identifiés comme appartenant à l'entreprise ont leur type de propriété configuré automatiquement en fonction de votre sélection. Vous pouvez ensuite configurer tous les terminaux personnels qui ne sont pas sur la liste afin de les enrôler avec un type de propriété personnel.

La procédure suivante explique comment importer la liste des terminaux professionnels préapprouvés. Vous pouvez appliquer automatiquement le type de propriété professionnel après l'enrôlement, même si une restriction applique automatiquement le type de propriété personnel.

Les restrictions pour un enrôlement ouvert, en revanche, autorisent ou bloquent explicitement l'enrôlement des terminaux dont les paramètres correspondent à ceux que vous indiquez, par exemple la plateforme, le modèle et le système d'exploitation.

1 Accédez à **Terminaux > Cycle de vie > Statut d'enrôlement** et sélectionnez **Ajouter**, puis **Importation par lot** pour afficher l'écran **Importation par lot**.

   Vous pouvez également sélectionner **Ajouter**, puis **Terminaux sur liste autorisée** pour saisir jusqu'à 30 terminaux sur liste autorisée à la fois par IMEI, UDID ou numéro de série. Vous pouvez également indiquer Professionnel ou Partagé comme **type de propriété**.

2 Entrez un **Nom de lot** et une **Description du lot**, puis sélectionnez **Ajouter un terminal sur liste autorisée** dans **Type de lot**.

3 Sélectionnez le lien « Télécharger le modèle avec un exemple pour les terminaux mis sur liste autorisée » et enregistrez ce modèle de valeurs séparées par des virgules (CSV, comma-separated values) dans un endroit auquel vous avez accès. Modifiez ce fichier CSV avec Excel pour ajouter tous les terminaux que vous souhaitez ajouter à la liste autorisée, puis enregistrez le fichier.

4 Sélectionnez **Choisir un fichier** et sélectionnez votre fichier CSV enregistré.

5 Sélectionnez **Importer** pour importer les informations sur le terminal dans votre liste autorisée.

6 Définissez le type de **Propriété par défaut du terminal** sur Personnel pour l'enrôlement libre.

   a Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement** et sélectionnez l'onglet **Regroupement**.

   b Sélectionnez **Personnel** comme **type de propriété de terminal par défaut**.

   c Sélectionnez le **rôle par défaut** attribué à l'utilisateur qui détermine son niveau d'accès au portail self-service (SSP).

   d Sélectionnez l'**action par défaut** pour les **utilisateurs inactifs**, ce qui détermine comment agir si l'utilisateur est marqué comme inactif.

   e Cliquez sur **Enregistrer**.

Demander aux utilisateurs d'identifier le type de propriété

Si votre déploiement dispose de plusieurs groupes organisationnels avec plusieurs types de propriété, vous pouvez demander aux utilisateurs d'identifier le type de propriété pendant l'enrôlement. Une attention particulière est nécessaire avant d'autoriser les utilisateurs à choisir leur propre type de propriété.

Cette approche est simple et suppose que chaque utilisateur sélectionne correctement le type de propriété qui s'applique à son terminal. Si un utilisateur de terminal personnel sélectionne par erreur le type Professionnel, son terminal est désormais assujetti à des politiques et à des profils qui ne s'appliquent pas normalement à des terminaux personnels. Cette sélection erronée peut avoir des répercussions légales sérieuses concernant la confidentialité de l'utilisateur.

Vous pouvez toujours mettre à jour le type de propriété de terminaux individuels ultérieurement, mais il est plus sûr d'établir la liste des terminaux professionnels. Enrôlez ensuite les terminaux professionnels séparément, puis définissez le type de propriété par défaut sur Personnel.

1 Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement** et sélectionnez l'onglet **Invite facultative**.

2 Cliquez sur **Demander le type de propriété du terminal**. Pendant l'enrôlement, il est demandé aux utilisateurs de sélectionner le type de propriété.

3 Cliquez sur **Enregistrer**.

Configurer les options d'enrôlement

Vous pouvez personnaliser votre workflow d'enrôlement en intégrant les options avancées disponibles dans Workspace ONE UEM.

Accédez aux autres options d'enrôlement en naviguant vers **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement**.

Démarrage

Paramètre	Description
Ajouter un domaine de messagerie	Ce bouton est utilisé pour configurer le service de détection automatique afin d'inscrire des domaines de messagerie à votre environnement.
Mode(s) d'authentification	Sélectionnez les types d'authentification autorisés, parmi lesquels : ■ **Basique** – Les comptes utilisateur basiques (ceux que vous créez manuellement dans UEM Console) peuvent s'enrôler. ■ **Annuaire** – Les comptes utilisateur d'annuaire (ceux que vous avez importés ou autorisés à l'aide de l'intégration des services d'annuaire) peuvent s'enrôler. L'enrôlement direct de Workspace ONE prend en charge les utilisateurs d'annuaire avec ou sans SAML. ■ **Proxy d'authentification** – Permet aux utilisateurs de s'enrôler à l'aide de comptes utilisateur Proxy d'authentification. Les utilisateurs s'authentifient auprès d'un point d'accès web. ■ Renseignez les champs **URL de proxy d'authentification**, **Sauvegarde de l'URL de proxy d'authentification** et **Type de méthode d'authentification** (faites votre choix entre HTTP de base et Exchange ActiveSync).
Source d'authentification pour Intelligent Hub	Sélectionnez le système que le service Intelligent Hub utilise comme source pour les utilisateurs et les stratégies d'authentification. ■ **Workspace ONE UEM** – Sélectionnez ce paramètre si vous voulez que les services du Hub utilisent Workspace ONE UEM en tant que source pour les utilisateurs et les stratégies d'authentification. Lorsque vous configurez la page **Configuration du Hub** pour les services du Hub, entrez l'URL du locataire des services du Hub. ■ **Workspace ONE Access** – Sélectionnez ce paramètre si vous souhaitez que les services du Hub utilisent Workspace ONE Access en tant que source pour les utilisateurs et les stratégies d'authentification. Lorsque vous configurez la page **Configuration du Hub** pour les services du Hub, entrez l'URL du locataire de Workspace ONE Access. Pour plus d'informations sur Workspace ONE Intelligent Hub, reportez-vous à la documentation sur VMware Workspace ONE Hub Services. Pour plus d'informations sur Workspace ONE Access, reportez-vous à la documentation sur VMware Workspace ONE Access.

Paramètre	Description
Mode d'enrôlement des terminaux	Sélectionnez le mode d'enrôlement des terminaux de votre préférence, notamment les options suivantes : ■ **Enrôlement ouvert** – Permet essentiellement à toute personne répondant aux autres critères d'enrôlement (mode d'authentification, restrictions, etc.) de s'enrôler. L'enrôlement direct de Workspace ONE prend en charge l'enrôlement ouvert. ■ **Terminaux enregistrés uniquement** – Autorise uniquement les utilisateurs à s'enrôler à l'aide de terminaux que vous ou eux avez inscrits. L'inscription des terminaux correspond au processus d'ajout de terminaux professionnels dans UEM Console avant leur enrôlement. L'enrôlement direct de Workspace ONE prend en charge l'autorisation d'enrôlement de terminaux enregistrés seulement, mais uniquement si les jetons d'enregistrement ne sont pas requis.
Exiger un jeton d'enregistrement	Visible uniquement lorsque l'option **Terminaux enregistrés uniquement** est sélectionnée. Si vous limitez l'enrôlement aux terminaux enregistrés, vous pouvez aussi demander qu'un jeton d'enregistrement soit utilisé pour l'enrôlement. Cette option offre davantage de sécurité car elle vous assure qu'un utilisateur en particulier est autorisé à s'enrôler. Vous pouvez envoyer un e-mail ou un SMS et joindre le jeton d'enrôlement pour les utilisateurs disposant d'un compte Workspace ONE UEM.
Exiger l'enrôlement par Intelligent Hub pour les terminaux iOS	Cochez cette case pour exiger que les utilisateurs des terminaux iOS téléchargent et installent Workspace ONE Intelligent Hub avant de pouvoir s'enrôler. Si elle est décochée, l'enrôlement par le Web est disponible.
Exiger l'enrôlement par Intelligent Hub pour les terminaux macOS	Cochez cette case pour exiger que les utilisateurs des terminaux macOS téléchargent et installent Workspace ONE Intelligent Hub avant de pouvoir s'enrôler. Si elle est décochée, l'enrôlement par le Web est disponible.

Configurer les options d'enrôlement sur l'intégration Hub

L'intégration Hub permet aux clients d'activer ou désactiver l'expérience des services du Hub à n'importe quel niveau du groupe organisationnel enfant dans l'arbre de groupe organisationnel.

Pour plus d'informations, reportez-vous à la documentation Workspace ONE Hub Services.

Paramètre	Description
Utiliser les fonctionnalités des services du Hub dans Intelligent Hub	Activez ce paramètre pour autoriser les terminaux de ce groupe organisationnel à se connecter aux services Workspace ONE Hub et disposer de fonctionnalités comme les onglets Catalogue d'applications unifié, Assistance, Notifications utilisateur final, People et Accueil. Désactivez ce paramètre pour que les terminaux adoptent le mode de gestion (mode Agent uniquement). Par exemple, utilisez Intelligent Hub et Workspace ONE Access, sans les fonctionnalités des services du Hub, pour l'authentification sur des terminaux durcis des branches d'activité.

Configurer les options d'enrôlement dans Conditions d'utilisation

L'onglet **Conditions d'utilisation** vous permet d'ajouter et d'examiner des conditions d'utilisation en ce qui concerne l'enrôlement. Accédez à l'onglet Invite facultative en naviguant vers **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement**.

Paramètre	Description
Exiger l'acceptation des conditions d'utilisation pour l'enrôlement	Activez ce paramètre pour exiger l'acceptation des conditions d'utilisation au moment de l'enrôlement.
Ajouter de nouvelles conditions d'utilisation d'enrôlement	Sélectionnez cette option pour lancer l'ajout de conditions d'utilisation aux fins de l'enrôlement.

Important Si vous activez **Exiger l'acceptation des conditions d'utilisation pour l'enrôlement**, vous devez créer des conditions d'utilisation. Sinon, les terminaux Windows Desktop risquent de ne pas parvenir à s'enrôler.

Configurer les options d'enrôlement dans l'onglet Regroupement

L'onglet Regroupement vous permet de visualiser et d'indiquer les informations de base relatives aux groupes organisationnels et aux ID de groupe pour les utilisateurs finaux. Activez le **mode d'attribution de l'ID de groupe** pour choisir comment l'environnement Workspace ONE UEM powered by AirWatch attribue des ID de groupe aux utilisateurs.

Accédez à l'onglet Regroupement en naviguant vers **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement**.

Paramètre	Description
Mode d'attribution de l'ID de groupe	L'enrôlement direct de Workspace ONE prend en charge tous les modes d'attribution. ■ **Par défaut** – Sélectionnez cette option si des ID de groupe à utiliser pour l'enrôlement sont fournis aux utilisateurs. L'ID de groupe utilisé détermine le groupe organisationnel attribué aux utilisateurs. ■ **Sélection manuelle de l'ID de groupe par l'utilisateur** – Activez cette option pour permettre aux utilisateurs des services d'annuaire de sélectionner un ID de groupe à partir d'une liste lors de l'enrôlement. La section **Attribution d'ID de groupe** répertorie tous les groupes organisationnels et les ID de groupe correspondants. Cette liste ne vous oblige pas à effectuer un mappage de l'attribution de groupes, mais l'utilisateur pourrait sélectionner un ID de groupe incorrect. ■ **Sélection automatique selon le groupe d'utilisateurs** – Cette option s'applique uniquement lors d'une intégration aux groupes d'utilisateurs. Activez cette option pour vous assurer que les utilisateurs sont automatiquement attribués aux groupes organisationnels en fonction de leurs attributions de groupe du service d'annuaire. La section **Paramètres d'attribution de groupe** répertorie tous les groupes organisationnels de l'environnement et les groupes d'utilisateurs du service d'annuaire correspondants. Cliquez sur le bouton **Modifier l'attribution du groupe** pour modifier les associations groupe organisationnel/groupe d'utilisateurs et définissez le rang de précédence pour chaque groupe. Par exemple, vous pourrez avoir trois groupes : Direction, Vente et Global qui sont classés par ordre de rôle de travail. Tout le monde est membre du groupe Global, donc si vous deviez mettre ce groupe d'utilisateurs au niveau supérieur, tous vos utilisateurs appartiennent à un seul groupe organisationnel. En revanche, si vous positionnez le groupe Direction en premier, vous vous assurez que les quelques employés qui lui appartiennent sont placés dans leur propre groupe organisationnel. En mettant le groupe Vente en seconde position, vous vous assurez que tous les employés appartenant à ce service sont regroupés dans un groupe organisationnel qui leur est dédié. Si vous mettez le groupe Global en troisième position, tout employé n'ayant pas été attribué à un groupe est placé dans un groupe organisationnel séparé.

Tableau 9-1. Par défaut

Paramètre	Description
Propriété par défaut du terminal	Sélectionnez la propriété du terminal par défaut pour l'enrôlement des terminaux dans le groupe organisationnel actuel. L'enrôlement direct de Workspace ONE prend en charge la définition d'une propriété de terminal par défaut.
Rôle par défaut	Sélectionnez les rôles par défaut attribués aux utilisateurs du groupe organisationnel actuel. Cela peut affecter l'accès au portail en libre-service. 1 **Accès complet** : accorde aux utilisateurs un accès aux fonctions SSP plus élevées (par exemple, installer/supprimer des profils et des applications, réinitialiser des codes secrets, envoyer des messages de terminaux et accéder en écriture au contenu). 2 **Accès basique** : accorde aux utilisateurs un accès à faible impact. Ils peuvent inscrire leurs propres terminaux, afficher les profils et les applications (mais pas les installer), afficher leur propre compte, et interroger et trouver leur propre terminal. 3 **Accès externe** : les utilisateurs avec un accès externe disposent de toutes les capacités en tant qu'utilisateurs à accès basique, mais bénéficient également d'un accès en lecture seule au contenu du SSP explicitement partagé avec eux. L'enrôlement direct de Workspace ONE prend en charge la définition d'un rôle par défaut.
Action par défaut pour les utilisateurs inactifs	Sélectionnez l'action par défaut qui aura un impact sur les utilisateurs Active Directory si leurs terminaux deviennent inactifs. Le traitement des comptes est toujours centré sur l'utilisateur plutôt que sur le terminal. Cela signifie que le comportement de traitement appliqué aux terminaux est basé sur les paramètres du OG où c'est l'**utilisateur** qui est géré, et non le terminal. L'enrôlement direct de Workspace ONE prend en charge la définition d'une action par défaut pour les utilisateurs inactifs.

Tableau 9-2. Synchroniser le groupe d'utilisateurs

Paramètre	Description
Synchroniser les groupes d'utilisateurs en temps réel pour Workspace ONE	Workspace ONE permet de synchroniser les groupes d'utilisateurs pour un utilisateur donné lorsqu'il s'enregistre auprès d'UEM Console. Cette fonction est activée par défaut. Elle est particulièrement efficace lorsque les groupes d'utilisateurs sont souvent utilisés pour les attributions d'applications, les attributions de profils, les attributions de politiques ou les mappages d'utilisateurs. Cette fonctionnalité est gourmande en ressources processeur. Par conséquent, vous devez désactiver ce paramètre, sauf si votre cas d'utilisation est similaire à la situation décrite, pour améliorer les performances et éviter les problèmes de latence lors du lancement de l'application Workspace ONE.

Tableau 9-3. Mappage du rôle utilisateur

Paramètre	Description
Activer le mappage du répertoire basé sur les groupes	Cochez cette case pour activer les attributions par classement qui relient un groupe d'utilisateurs du répertoire à un rôle Workspace ONE UEM spécifique. Les utilisateurs appartenant à un groupe particulier se voient attribuer les rôles associés. S'ils appartiennent à plusieurs groupes, ils reçoivent le couplage le mieux classé. Vous pouvez modifier l'ordre de classement des groupes d'utilisateurs auxquels correspond un rôle en cliquant sur le bouton **Modifier l'attribution**. L'enrôlement direct de Workspace ONE prend en charge le mappage basé sur des groupes d'annuaire.

Configurer les options d'enrôlement dans l'onglet Invite facultative

Dans l'onglet **Invite facultative**, vous pouvez décider de demander des informations supplémentaires sur le terminal ou d'afficher des messages facultatifs contenant des informations de MDM et d'enrôlement.

Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement** et sélectionnez l'onglet **Invite facultative**.

Vous trouverez des instructions spécifiques à la configuration des messages, des modèles et des notifications après le tableau ci-dessous.

Paramètre	Description
Demander le type de propriété du terminal	Vous pouvez inviter l'utilisateur à sélectionner le type de propriété de son terminal. Sinon, configurez un type de propriété par défaut pour le groupe organisationnel actuel. L'enrôlement direct de Workspace ONE prend en charge la demande de type de propriété de terminal.
Afficher le message de bienvenue	Vous pouvez afficher un message de bienvenue pour vos utilisateurs au début du processus d'enrôlement du terminal. Vous pouvez configurer l'en-tête et le corps de ce message d'accueil en accédant à **Système > Localisation > Gestionnaire de localisation**. Ensuite, sélectionnez les libellés EnrollmentWelcomeMessageHeader et EnrollmentWelcomeMessageBody respectivement.
Afficher un message d'installation MDM	Vous pouvez afficher un message pour vos utilisateurs au début du processus d'enrôlement du terminal. Vous pouvez configurer l'en-tête et le corps de ce message d'installation MDM en accédant à **Système > Localisation > Gestionnaire de localisation**. Sélectionnez ensuite les libellés EnrollmentMdmInstallationMessageHeader et EnrollmentMdmInstallationMessageBody respectivement. Si vous choisissez de rédiger vos propres en-têtes et corps du message à l'aide du gestionnaire de localisation, vous devez sélectionner Remplacer dans l'option **Paramètre actuel**. Cela permet l'utilisation de vos textes personnalisés à la place des messages par défaut. En plus d'apporter des modifications ponctuelles à la localisation, vous pouvez également apporter des modifications de localisation en masse en téléchargeant un fichier de valeurs séparées par des virgules (CSV, comma-separated values) modifié. Téléchargez ce fichier CSV de modèles de localisation en accédant à **Système > Localisation > Gestionnaire de localisation** et sélectionnez le bouton **Modifier**. Modifiez le fichier selon vos préférences pour affecter des modifications de localisation en masse et importez-le à partir du même écran.

Paramètre	Description
Activer la demande de l'e-mail d'enrôlement	Vous pouvez inviter l'utilisateur à saisir ses identifiants pendant l'enrôlement. la demande d'e-mail d'enrôlement exige l'adresse e-mail de l'utilisateur final afin de remplir automatiquement cette option dans le profil de l'utilisateur. Ces données sont particulièrement intéressantes pour les organisations déployant les e-mails vers les terminaux en utilisant la valeur de recherche {EmailAddress}.
Activer la demande du numéro d'actif	Vous pouvez inviter l'utilisateur à saisir le numéro d'actif du terminal pendant l'enrôlement. L'enrôlement direct de Workspace ONE prend en charge les invites d'enrôlement par e-mail, mais seulement lorsque l'option **Demander le type de propriété du terminal** est activée et uniquement pour les terminaux professionnels.
Afficher les messages de transition d'enrôlement (sur Android seulement)	Vous pouvez afficher ou masquer les messages d'enrôlement sur les terminaux Android.
Activer la page de suivi d'état pour OOBE	Activez ce paramètre pour afficher la page de suivi d'état lors de l'enrôlement OOBE (Out of Box Enrollment) qui affiche l'état de provisionnement du terminal et indique à l'utilisateur les applications, les ressources et les stratégies qui ont été installées.
Autoriser l'authentification manuelle TLS pour Windows	Vous pouvez forcer les terminaux Windows à utiliser des points de terminaison sécurisés par l'authentification mutuelle TLS qui nécessite une installation et une configuration supplémentaires. Contactez le support technique pour obtenir de l'aide.
Afficher le message de l'écran d'authentification (Windows uniquement)	Vous pouvez fournir aux utilisateurs finaux de votre terminal un conseil de connexion personnalisé sur ce qu'ils doivent utiliser pour s'enrôler dans Workspace ONE UEM Console. Par exemple, si l'authentification d'enrôlement pour UEM est la même que les informations d'identification d'Active Directory, vous pouvez l'inclure comme conseil. Vous pouvez également inclure un lien sur lequel ils peuvent cliquer pour obtenir de l'aide. Cette fonctionnalité n'est actuellement prise en charge que par les terminaux Windows. Vous devez fournir votre propre localisation en incluant des traductions du conseil dans la même zone de texte.

Créer un message d'enrôlement personnalisé

Vous pouvez personnaliser les messages liés à l'enrôlement d'un terminal et toutes les autres invites liées au MDM envoyées vers un terminal.

1 Accédez à **Terminaux > Paramètres des terminaux > Général > Enrôlement** et sélectionnez l'onglet **Personnalisation**.

2 Sélectionnez **Utiliser un modèle de message spécifique pour chaque plateforme** et choisissez un modèle de message d'activation du terminal à partir du menu déroulant correspondant à chaque plateforme. Créez un nouveau modèle de message en suivant les étapes de la section **Créer des modèles de message** sous cette section.

3 Pour les terminaux iOS, vous pouvez configurer les éléments suivants, si vous le souhaitez.

   a Saisissez une **URL de redirection après l'enrôlement** (pour les terminaux iOS).

   b Saisissez un **message de profil MDM** qui apparaîtra dans l'invite d'installation du profil MDM lors de l'enrôlement (pour les terminaux iOS).

4 Cliquez sur **Enregistrer**.

Création de modèles de message

Créez votre propre bibliothèque de modèles de message personnalisés selon la plateforme pour couvrir la variété de scénarios que vous pourriez rencontrer.

1 Accédez à **Terminaux > Paramètres des terminaux > Général > Modèles de message**, puis cliquez sur **Ajouter**.

2 Définissez la **catégorie** de sorte qu'elle corresponde à votre modèle. Les options comprennent : **Administrateur**, **Application**, **Conformité**, **Contenu**, **Cycle de vie du terminal**, **Enrôlement** et **Conditions d'utilisation**.

3 Définissez le **type** qui correspond le mieux à la sous-catégorie. Les options du menu **Type** dépendront des paramètres du champ **Catégorie**.

4 Cliquez sur le menu **Sélectionner la langue**. Seules les langues définies dans les paramètres régionaux actifs sont affichées. Sélectionnez le bouton **Ajouter** pour ajouter des langues.

5 Vous pouvez cocher la case **Par défaut** si vous voulez que ce modèle soit l'option par défaut pour la **catégorie** sélectionnée.

6 Sélectionnez le **type de message** pour le modèle. Les options sont les suivantes : **E-mail**, **SMS*** et Notification **Push**.

7 Rédigez votre message **e-mail** en saisissant le texte dans le champ **Corps du message**.

- L'option de **texte brut** présente simplement une police sérif à espacement (Courier) sans option de mise en forme.
- L'option **HTML** active un format **RTF** qui permet de modifier notamment la police, la mise en forme, les titres, les puces, le retrait, la justification des paragraphes, les indices, les exposants, les images et les liens hypertextes. L'environnement HTML prend en charge le codage HTML basique à l'aide du bouton **Afficher la source** qui vous permet de basculer entre le **format RTF** et l'affichage source.

8 Sauvegardez votre modèle en cliquant sur **Enregistrer**.

* Pour que les notifications SMS fonctionnent avec votre flotte de terminaux, vous devez avoir un compte auprès d'un fournisseur de passerelle tiers et configurer les paramètres de passerelle. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > SMS** et renseignez les options décrites dans Paramètres des SMS.

Configurer les notifications du cycle de vie

Les notifications relatives au cycle de vie vous permettent de distribuer des messages personnalisés après certains événements se produisant au cours du cycle de vie d'un terminal, y compris l'enrôlement et le désenrôlement.

Vous pouvez configurer ce paramètre facultatif en accédant à **Terminaux > Cycle de vie > Paramètres > Notifications** et en complétant les options des sections suivantes.

- **Terminal désenrôlé** – Envoyez une notification par e-mail lorsqu'un terminal a été désenrôlé.
- **Terminal enrôlé** – Envoyez une notification par e-mail lorsque l'enrôlement d'un terminal a réussi.
- **Terminal bloqué en raison d'une restriction d'enrôlement** – Envoyez une notification par e-mail si une restriction d'enrôlement bloque un terminal. Vous pouvez configurer ce comportement en naviguant vers **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et en cliquant sur l'onglet **Restrictions**.

Paramètre	Description
Envoyer un e-mail à.	■ **Aucun(e)** – Choisissez cette option pour ne pas envoyer d'e-mails de confirmation lors de la réussite de l'enrôlement, du désenrôlement ou du blocage du terminal. ■ **Utilisateur** – Envoyez un e-mail de confirmation à l'utilisateur du terminal pour l'informer de la réussite de l'enrôlement, du désenrôlement ou du blocage du terminal. ■ **Cc** – Envoyez le même e-mail de confirmation à une seule ou à plusieurs adresses e-mail, séparées par des virgules. ■ **Modèle de message** – Sélectionnez le modèle de message de votre choix dans la liste déroulante. Vous pouvez ajouter un nouveau modèle de message ou en modifier un existant en sélectionnant le lien hypertexte « Cliquer ici… » qui vous dirige vers la page de paramètres **Terminaux et utilisateurs > Général > Modèles de message**. ■ **Administrateur** – Envoyez un e-mail de confirmation à l'administrateur Workspace ONE UEM pour l'informer de la réussite de l'enrôlement, du désenrôlement ou du blocage du terminal. ■ **À** – Envoyez le même e-mail de confirmation à une seule ou à plusieurs adresses e-mail, séparées par des virgules.

Configurer les options d'enrôlement dans l'onglet Personnalisation

Vous pouvez offrir à l'utilisateur un niveau supplémentaire de support, comprenant l'adresse e-mail et le numéro de téléphone, en configurant l'onglet **Personnalisation**. Un tel niveau de support est intéressant si les utilisateurs ne peuvent pas enrôler leurs terminaux, pour quelque raison que ce soit.

Accédez à l'onglet Personnalisation en naviguant vers **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement**.

Paramètre	Description
Utiliser un modèle de message spécifique pour chaque plateforme	Si cette option est activée, vous pouvez sélectionner un modèle de message unique pour chaque plateforme. Le lien fourni affiche la page Modèle de message, vous permettant de créer immédiatement des modèles. L'enrôlement direct de Workspace ONE™ prend en charge les modèles de message propres à la plateforme.
E-mail de support pour l'enrôlement	Saisissez l'adresse e-mail.

Paramètre	Description
Numéro de téléphone de support pour l'enrôlement	Saisissez le numéro de téléphone.
URL de redirection après l'enrôlement (iOS uniquement)	Vous pouvez fournir une URL de redirection vers la page d'accueil une fois l'enrôlement réussi. Cette URL peut être une ressource d'entreprise, comme le site Internet de l'entreprise ou l'écran de connexion pour les ressources supplémentaires. L'enrôlement direct de Workspace ONE prend en charge les URL de redirection après l'enrôlement.
Message de profil MDM (iOS uniquement)	Cette zone de texte est destinée au message qui s'affiche pendant l'enrôlement, pour les terminaux iOS uniquement. Vous pouvez saisir un message de 255 caractères maximum. L'enrôlement direct de Workspace ONE prend en charge les messages de profil MDM pour iOS uniquement.
Utiliser les applications MDM personnalisées	Affiche un lien qui ouvre la page Liste de groupes d'applications. Ce lien est intitulé **Groupes d'applications**. L'enrôlement direct de Workspace ONE prend en charge les applications MDM personnalisées.

Enregistrement des terminaux sur liste bloquée et liste autorisée

Une liste bloquée établit explicitement les terminaux ou les applications non autorisés. Une liste autorisée répertorie uniquement les terminaux ou les applications autorisés. Appliquez ce concept à l'enregistrement et vous pourrez contrôler les terminaux autorisés à s'enrôler dans Workspace ONE UEM powered by AirWatch.

Par exemple, lors d'un déploiement de terminaux professionnels uniquement, vous pouvez créer une liste autorisée pour les terminaux iOS approuvés. Vous pouvez baser cette liste de terminaux sur leur IMEI, leur numéro de série ou leur identificateur unique (UDID). Ainsi, l'enrôlement est limité aux terminaux que vous avez identifiés et l'enrôlement des terminaux personnels des employés ne sera pas possible.

En outre, si un terminal est perdu ou volé, vous pouvez ajouter son IMEI, son numéro de série ou ses informations UDID à la liste bloquée des terminaux. En mettant un terminal sur liste bloquée, vous désenrôlez le terminal et supprimez tous les profils MDM jusqu'à ce qu'il soit retiré de la liste bloquée.

Le dossier d'enregistrement d'un utilisateur est mis à jour avec les informations sur le terminal après l'enrôlement. Lorsque le terminal n'est pas enrôlé, tout autre utilisateur tentant d'enrôler le même terminal est bloqué de l'enrôlement tant que le dossier d'enregistrement de l'utilisateur précédent n'est pas supprimé.

Ajouter un terminal sur liste bloquée ou autorisée

Vous pouvez ajouter un terminal mis sur liste bloquée (interdit d'enrôlement) ou sur liste autorisée (autorisé à s'enrôler) en fonction des différents attributs de terminaux.

Note La mise sur liste bloquée des terminaux enregistrés dans le programme d'enrôlement des terminaux (DEP) empêche qu'un profil DEP leur soit attribué à l'avenir.

1 Accédez à **Terminaux > Cycle de vie > Statut de l'enrôlement** et cliquez sur **Ajouter**.

2 Sélectionnez **Terminaux sur liste bloquée** ou **Terminaux sur liste autorisée** dans la liste déroulante **Ajouter** et définissez les paramètres.

Paramètre	Description
Terminaux sur liste bloquée/autorisée	Saisissez les terminaux mis sur liste bloquée ou sur liste autorisée (grâce à la sélection Attribut du terminal), jusqu'à 30 à la fois.
Attribut du terminal	Sélectionnez le type d'attribut du terminal correspondant. Sélectionnez IMEI, Numéro de série ou UDID.
Groupe organisationnel	Confirmez le groupe organisationnel concerné par la liste bloquée ou autorisée de terminaux.
Propriété	Vous pouvez autoriser uniquement les terminaux correspondant au type de propriété sélectionné. Cette option est uniquement disponible pour les terminaux mis sur liste autorisée.
Informations supplémentaires	Elles vous permettent de sélectionner une plateforme pour appliquer votre liste bloquée ou autorisée.
Plateforme	Vous pouvez mettre sur liste bloquée ou sur liste autorisée tous les terminaux appartenant à la plateforme. Cette option n'est disponible que lorsque la case **Informations supplémentaires** est cochée.

3 Cliquez sur **Enregistrer** pour confirmer les paramètres.

Enregistrement du terminal

Enregistrer les terminaux d'entreprise est facultatif. L'avantage principal de cette option réside dans la restriction de l'enrôlement dans Workspace ONE UEM aux terminaux enregistrés uniquement.

Avantages de l'enregistrement

En plus de permettre la limitation de l'enrôlement aux terminaux inscrits, l'enregistrement présente l'avantage de pouvoir suivre les états d'enrôlement. Vous savez ainsi quels sont vos utilisateurs qui se sont enrôlés et quels sont ceux qui ne l'ont pas encore fait. Vous pouvez alors informer les utilisateurs qui ne sont pas encore enrôlés.

Workspace ONE UEM peut inscrire les terminaux même lorsqu'il manque des identifiants de terminaux lors de la phase de saisie des données, par les utilisateurs ou les administrateurs.

La sécurité constitue un troisième avantage de l'inscription des terminaux avant l'enrôlement. Un terminal inscrit s'attend à ce que l'utilisateur qui se connecte pour la première fois soit la personne pour laquelle il a été inscrit. Si un autre utilisateur tente de se connecter à un terminal inscrit, ce dernier est verrouillé et ne peut pas s'enrôler.

Éléments à prendre en compte pour l'enrôlement

Si vous souhaitez enregistrer les terminaux avant de les enrôler, prenez en compte les éléments suivants.

Qui inscrira les terminaux ?

Ceci est important à prendre en compte lorsque l'inscription des terminaux décide qui l'effectue.

- Quel est le nombre total de terminaux pour votre déploiement ? Dans les déploiements de plusieurs milliers de terminaux, vous pouvez ajouter ces informations dans un fichier de valeurs séparées par des virgules (CSV, comma-separated values). Vous téléchargez ensuite ce fichier avant que les terminaux soient provisionnés. Consultez les sections intitulées **Inscrire un terminal individuel** et **Inscrire plusieurs terminaux** sur cette page.
- Prenez-vous en charge un programme BYOD permettant aux employés d'utiliser leurs terminaux personnels. Si vous choisissez de limiter l'enrôlement aux terminaux inscrits uniquement, vous pouvez donner des consignes aux employés pour qu'ils inscrivent leurs terminaux. Consultez la section suivante intitulée **Inscription des terminaux par l'utilisateur via le SSP** sur cette page.

Inscription des terminaux par l'utilisateur via le SSP

Vous pouvez diriger les utilisateurs vers l'inscription de leurs propres terminaux avant leur enrôlement dans Workspace ONE UEM si vous prenez en charge les terminaux BYOD. Vous pouvez également demander aux utilisateurs de terminaux professionnels de les inscrire si vous voulez suivre leur enrôlement ou bien d'utiliser des jetons d'enregistrement. Dans les deux cas, vous devez notifier vos utilisateurs du processus à suivre.

Les consignes suivantes impliquent que l'utilisateur dispose d'identifiants Workspace ONE UEM issus de son service d'annuaire actuel ou d'un compte utilisateur précédemment activé. Si vous avez opté pour un enrôlement avec les services d'annuaire sans ajouter manuellement les utilisateurs, vous n'aurez pas de compte utilisateur créé.

Dans ce cas, si vous voulez que les utilisateurs inscrivent leurs terminaux, vous devez envoyer un e-mail ou une notification intranet à chaque groupe d'utilisateurs extérieur à Workspace ONE UEM pour leur donner les consignes d'inscription. Assurez-vous que l'authentification d'enrôlement est activée pour Active Directory ou pour le serveur proxy d'authentification en accédant à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement > Authentification**.

Vérifiez également que la case **Bloquer les utilisateurs inconnus** est décochée en accédant à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement > Restrictions**.

- Envoyez un e-mail ou une notification intranet aux utilisateurs en dehors de Workspace ONE UEM avec les informations d'inscription.
- Vous pouvez créer des comptes utilisateur pour que tous les utilisateurs finaux inscrivent leurs terminaux, puis envoyer des messages d'activation de compte utilisateur à chacun, avec les instructions d'inscription.

Incluez ces cinq étapes dans le message d'inscription que vous envoyez aux utilisateurs finaux, afin qu'ils reçoivent les éléments dont ils ont besoin pour inscrire leurs propres terminaux.

1 Accédez à l'URL du Portail en libre-service (SSP) : **https://<UEM_Environment>/MyDevice**, où <UEM_Environment> représente l'URL d'enrôlement pour votre environnement.

2 Saisissez l'**ID de groupe** et les identifiants – une adresse e-mail ou un nom d'utilisateur et mot de passe.

   Ces identifiants peuvent correspondre aux identifiants du service d'annuaire pour les utilisateurs d'annuaire.

3 Cliquez sur **Ajouter des horaires** pour ouvrir le formulaire **Inscrire un terminal**.

4 Saisissez les informations du terminal en complétant les zones de texte du formulaire **Inscrire un terminal**.

5 Envoyez les informations et sélectionnez **Enregistrer** pour inscrire le terminal.

Limiter l'enrôlement aux terminaux inscrits uniquement

A ce stade, vous pouvez limiter l'enrôlement aux terminaux inscrits uniquement, que les administrateurs ou les utilisateurs aient enregistré leurs terminaux ou non. Pour ce faire, accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement** et sélectionnez **Terminaux enregistrés uniquement**.

Suivre l'état d'enrôlement

Vous devrez peut-être occasionnellement résoudre des problèmes liés à l'inscription d'un terminal ou suivre l'avancée du processus d'enrôlement global. Les utilisateurs finaux pourraient accidentellement supprimer le message contenant les instructions d'inscription ou ne pas s'authentifier avant l'expiration de la période allouée.

Une fois les terminaux inscrits, vos pouvez suivre les statuts d'enrôlement en naviguant vers la page **Tableau de bord des terminaux** et en sélectionnant le tableau **Enrôlement** qui vous permet de filtrer en fonction du statut. Vous pouvez également accéder au Monitor qui liste les terminaux récemment enrôlés.

Gérez l'état d'enrôlement en accédant à la page État d'enrôlement sous **Terminaux > Cycle de vie > État d'enrôlement**. Suivez le statut d'enrôlement des terminaux en triant la colonne **Statut d'enrôlement** ou bien en filtrant l'affichage en liste par **Statut d'enrôlement**.

En utilisant la page Statut d'enrôlement, vous pouvez produire une liste personnalisée des terminaux inscrits (mais non enrôlés), sélectionnez tous les terminaux dans cette liste personnalisée et renvoyez les instructions d'enrôlement. Si le temps écoulé est suffisant et qu'un appareil ne parvient pas à s'enrôler, vous pouvez choisir de réinitialiser (ou même de révoquer) son jeton d'enregistrement.

Pour plus d'informations, consultez la section État de l'enrôlement.

Synchronisation d'un groupe d'utilisateurs lors de l'enrôlement

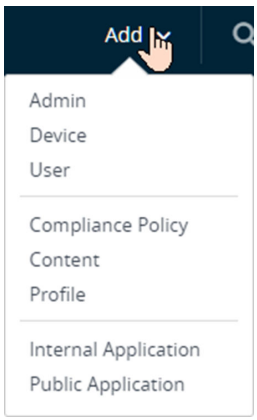
Si vous avez l'intention d'organiser les attributions d'applications, les attributions de profils de terminaux, les attributions de politiques de conformité ou les mappages des utilisateurs autour de groupes d'utilisateurs, vous pouvez maintenir activé le paramètre Synchroniser le groupe d'utilisateurs, ce qui est son état par défaut. Ce paramètre permet à Workspace ONE de passer un appel en temps réel au serveur d'authentification à chaque fois qu'un enregistrement de terminal est créé.

Pour plus d'informations, consultez la section **Synchroniser le groupe d'utilisateurs** dans Configurer les options d'enrôlement dans l'onglet Regroupement.

Inscrire un terminal individuel

Lorsque vous avez un petit nombre de terminaux à inscrire, vous pouvez les inscrire individuellement.

1 Cliquez sur le bouton **Ajouter** qui se trouve dans le quadrant supérieur droit de la plupart des écrans de Workspace ONE UEM Console. Lorsque ce bouton est sélectionné, il affiche un menu déroulant avec plusieurs options.



2 Sélectionnez **Terminal**.

La page **Ajouter un terminal** s'affiche.

3 Définissez les options en fonction de vos besoins, en commençant par l'onglet **Utilisateur**.

Paramètre	Description
Section Utilisateur	
Texte recherché	Recherchez l'utilisateur en saisissant un paramètre de recherche et cliquez sur **Rechercher un utilisateur**. Lors d'une recherche réussie, sélectionnez le compte utilisateur pour lequel vous enregistrez le terminal. Plusieurs zones de texte pré-remplies s'affichent, notamment Type de sécurité, Nom d'utilisateur, Mot de passe et Adresse e-mail. Vous pouvez les modifier en affichant les détails avancés.
Section Terminal	
Nom convivial attendu	Saisissez le nom convivial du terminal. Cette zone de texte accepte les **valeurs de recherche** que vous pouvez insérer en cliquant sur le signe Plus. Pour plus d'informations, reportez-vous à la section Chapitre 12 Valeurs de recherche.
Groupe organisationnel	Sélectionnez le groupe organisationnel auquel le terminal appartient.
Propriété	Sélectionnez le type de propriété du terminal.
Plateforme	Sélectionnez la plateforme du terminal.
Afficher les options avancées d'informations du terminal	Affichez les paramètres avancés d'informations du terminal.
Modèle	Sélectionnez le modèle du terminal. Les options du menu déroulant dépendent de la **plateforme** sélectionnée.
OS	Sélectionnez le système d'exploitation du terminal. Les options du menu déroulant dépendent de la **plateforme** sélectionnée.
UDID*	Saisissez l'UDID du terminal.
Numéro de série* ‡	Saisissez le numéro de série du terminal.
IMEI*	Saisissez le numéro IMEI du terminal.
SIM*	Saisissez le numéro de SIM du terminal.
Numéro d'actif*	Saisissez le numéro d'actif du terminal.
Section Messagerie	
Type de message	Type de notification envoyée à l'utilisateur une fois le terminal ajouté. Faites votre choix entre **Aucun(e)**, **E-mail** ou **SMS***. L'option E-mail nécessite une adresse e-mail valide. Vous devez également sélectionner un modèle d'e-mail. L'option SMS nécessite un numéro de téléphone comprenant l'indicatif pays et l'indicatif régional. Des frais peuvent s'appliquer. Vous devez également sélectionner un modèle de message SMS.
Adresse e-mail	Requise pour le type de message E-mail.
Modèle d'e-mail	Requise pour le type de message E-mail. Sélectionnez un modèle dans le menu déroulant. Affichez l'e-mail en cliquant sur le bouton **Aperçu du message**.

Paramètre	Description
Numéro de téléphone	Requis pour le type de message SMS*.
Modèle de SMS	Requis pour le type de message SMS*. Sélectionnez un modèle dans la liste déroulante. Affichez le SMS en cliquant sur **Aperçu du message**.

* Pour que les notifications SMS fonctionnent avec votre flotte de terminaux, vous devez avoir un compte auprès d'un fournisseur de passerelle tiers et configurer les paramètres de passerelle. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > SMS** et renseignez les options décrites dans Paramètres des SMS.

* Vous devez en remplir au moins un des paramètres signalés pour inscrire votre terminal.

‡ Pour inscrire un terminal Windows Desktop, vous devez saisir son numéro de série.

4 (Facultatif) Renseignez l'onglet **Attributs personnalisés**.

Paramètre	Description
Ajouter	Ajoutez un **Attribut** personnalisé ainsi que son **Application** et sa **Valeur** correspondantes en sélectionnant ce bouton. Pour pouvoir utiliser la fonctionnalité d'attribut personnalisé lors de l'ajout d'un terminal, vous devez avoir déjà créé un attribut personnalisé. Pour ce faire, reportez-vous à la section Chapitre 5 Attributs personnalisés.
Application	Sélectionnez l'application qui collecte l'attribut.
Attributs	Sélectionnez l'attribut personnalisé dans le menu déroulant.
Valeur	Sélectionnez l'attribut personnalisé dans le menu déroulant.

5 (Facultatif) Renseignez l'onglet **Étiquettes**.

Paramètre	Description
Ajouter	Ajouter une **balise** au terminal
Balise	Sélectionnez la balise dans le menu déroulant de balises existantes.

6 Cliquez sur **Enregistrer** pour terminer le processus d'inscription du terminal.

Résultat : le terminal est maintenant enregistré pour le compte utilisateur Workspace ONE UEM sélectionné défini à l'étape 3.

Que faire ensuite ? Remettez ce terminal à cet utilisateur afin qu'il puisse se connecter et terminer le processus d'enrôlement. Si un autre utilisateur tente de se connecter à ce terminal avant l'utilisateur enregistré, le terminal est verrouillé et ne peut pas s'enrôler.

Inscription de plusieurs terminaux

Si vous avez un grand nombre de terminaux à inscrire, le processus d'importation par lot est la meilleure façon de procéder.

1 Accédez à **Comptes > Utilisateurs > Affichage en liste** ou **Terminaux > Cycle de vie > Statut d'enrôlement**.

   a Sélectionnez **Ajouter**, puis **Importation par lots** pour afficher l'écran **Importation par lots**.

2 Complétez chacune des options requises : **Nom du lot**, **Description du lot** et **Type de lot**.

   Dans l'option **Fichier d'importation par lots (.csv)** se trouve une liste de modèles de tâches que vous pouvez utiliser pour charger en masse les utilisateurs et leurs terminaux.

3 Sélectionnez le modèle de téléchargement approprié et enregistrez le fichier de valeurs séparées par des virgules (CSV, comma-separated values) dans un emplacement accessible.

4 Localisez le fichier CSV enregistré, ouvrez-le avec Excel et saisissez les informations pertinentes pour chacun des terminaux à importer.

   Chaque modèle comporte des textes par défaut illustrant le type d'informations (et leur format) destinées à être saisies dans chaque colonne. Les champs du fichier CSV marqués d'un astérisque (*) sont obligatoires.

5 Enregistrez le modèle complété en tant que fichier CSV. Dans UEM Console, sélectionnez le bouton **Choisir un fichier** dans l'écran **Importation par lots**, naviguez jusqu'à l'emplacement où vous avez enregistré le fichier CSV complété et sélectionnez-le.

6 Cliquez sur **Enregistrer** pour terminer l'inscription pour tous les utilisateurs listés et les terminaux correspondants.

Jetons d'enregistrement

Si vous limitez l'enrôlement aux terminaux enregistrés, vous pouvez aussi demander un jeton d'enregistrement. Cette option offre davantage de sécurité car elle vous assure qu'un utilisateur en particulier est autorisé à s'enrôler.

Vous pouvez envoyer un e-mail ou un SMS et joindre le jeton d'enrôlement pour les utilisateurs disposant d'un compte Workspace ONE UEM.

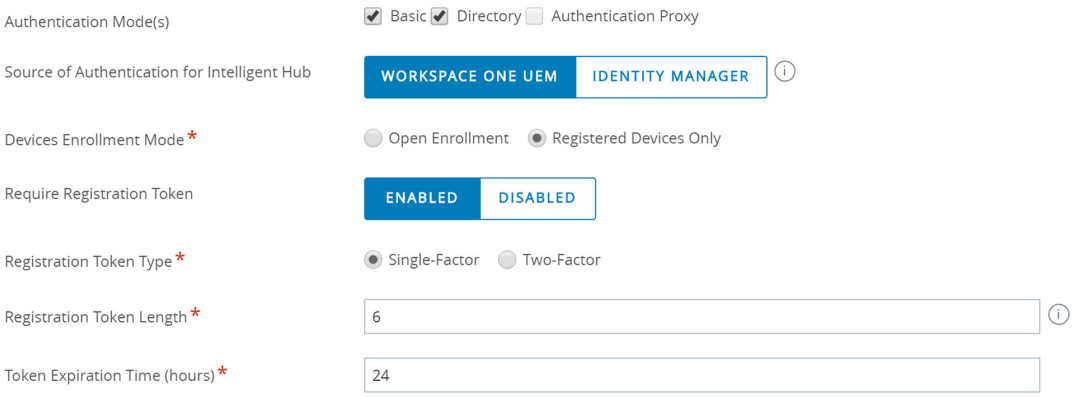
Note Pour que les notifications SMS fonctionnent avec votre flotte de terminaux, vous devez avoir un compte auprès d'un fournisseur de passerelle tiers et configurer les paramètres de passerelle. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > SMS** et renseignez les options décrites dans Paramètres des SMS.

Activer le jeton d'enregistrement

1 Activez un enrôlement basé sur les jetons en sélectionnant le groupe organisationnel approprié. Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Enrôlement** et assurez-vous de sélectionner l'onglet **Authentification**.

2 Faites défiler l'affichage jusqu'à la fin de la section **Assistant de démarrage** et sélectionnez **Terminaux enregistrés uniquement** comme **Mode d'enrôlement des terminaux**.

Un curseur intitulé **Exiger un jeton d'enregistrement** apparaît. L'activation de cette option limite l'enrôlement aux terminaux enregistrés par jeton.



3 Sélectionnez un **type de jeton d'enregistrement**. Les choix sont les suivants :

- **Facteur unique** – Le jeton suffit à l'enrôlement.
- **Deux facteurs** – Un jeton et une connexion avec les identifiants de l'utilisateur sont nécessaires à l'enrôlement.

4 Définissez la **longueur du jeton d'enregistrement**.

Ce paramètre obligatoire indique la complexité du jeton d'enregistrement ainsi que sa longueur comprise entre 6 et 20 caractères alphanumériques.

5 Définissez le **délai d'expiration du jeton** (en heures).

Ce paramètre obligatoire indique la durée dont dispose l'utilisateur pour sélectionner le lien et s'inscrire. Une fois expiré, un autre lien doit être envoyé.

Générer un jeton

Vous devez générer et envoyer un jeton d'enregistrement, qui est une méthode hautement sécurisée d'enrôlement d'un terminal mobile. Il existe deux façons de générer un jeton : via **UEM Console** ou via le **Portail en libre-service**.

UEM Console	Portail en libre-service
1 Accédez à **Comptes > Utilisateurs > Affichage en liste** et sélectionnez **Modifier l'utilisateur**. La page Ajouter/ Modifier l'utilisateur s'affiche. 2 Faites défiler vers le bas et cliquez sur **Type de message.** Les choix sont les suivants : ■ **E-mail** pour les utilisateurs des services d'annuaire ■ **SMS** pour les comptes d'utilisateurs de base 3 Sélectionnez le **modèle de message**. Cliquez ensuite sur **Enregistrer et ajouter un terminal**. L'écran **Ajouter un terminal** s'affiche. Vous pouvez utiliser le modèle par défaut ou en créer un en cliquant sur le lien ci-dessous qui ouvre la page de **modèle de message** dans un nouvel onglet. 4 Vérifiez les informations **générales** relatives au terminal ainsi que celles du **message** lui-même. Une fois que vous avez terminé, cliquez sur **Enregistrer** pour envoyer le jeton à l'utilisateur utilisant le type de message sélectionné. **Note** pour des raisons de sécurité, le jeton n'est pas accessible dans UEM Console.	1 Connectez-vous au portail self-service. Si vous utilisez l'accès SSO ou les cartes à puce pour l'authentification, vous pouvez vous connecter depuis un terminal ou un ordinateur. Les utilisateurs d'annuaire peuvent se connecter avec leurs identifiants de service d'annuaire. 2 Cliquez sur **Ajouter un terminal**. 3 Saisissez les informations du terminal (nom convivial et plateforme) et tout autre détail en renseignant les paramètres du formulaire **Inscrire un terminal**. Assurez-vous que le numéro de téléphone et l'adresse e-mail sont correctement renseignés, car ils pourraient ne pas être remplis automatiquement. 4 Cliquez sur **Enregistrer** pour envoyer le jeton à l'utilisateur utilisant le type de message sélectionné. **Note** Le jeton ne s'affiche pas sur cette page, mais seulement dans le message envoyé. Comme fonctionnalité de sécurité, les modifications suivantes ont été apportées aux comptes enrôlés avec un jeton. ■ L'adresse e-mail et le numéro de téléphone sur les écrans **Ajouter un terminal** et **Compte** sont en lecture seule. ■ L'action Afficher le message d'enrôlement a été supprimée.

Instructions destinées aux utilisateurs qui s'enrôlent avec un jeton

Vos utilisateurs peuvent utiliser un jeton d'enregistrement pour enrôler un terminal, une méthode d'authentification hautement sécurisée.

1 Ouvrez l'e-mail ou le SMS sur le terminal et cliquez sur le lien qui contenant le jeton d'enrôlement. Si une page d'enrôlement vous demande de saisir une ID de groupe ou un jeton, saisissez directement le jeton.

2 Dans le cas d'une authentification à deux facteurs, saisissez un nom d'utilisateur et un mot de passe.

3 Poursuivez votre enrôlement comme d'habitude.

Résultat : une fois que vous avez terminé, le terminal est associé à l'utilisateur pour lequel le jeton a été créé.

Que faire ensuite ? Une fois le profil MDM installé sur le terminal, le jeton est considéré comme étant « utilisé » et ne peut pas l'être pour enrôler d'autres terminaux. Si l'enrôlement n'est pas terminé, le jeton peut encore être utilisé sur un autre terminal. Si le jeton expire après la durée que vous avez indiquée, vous devez générer un autre jeton d'enrôlement.

Identificateur de terminal manquant lors de l'inscription

Si aucun identificateur de terminal n'est indiqué lors de l'inscription (UDID, IMEI ou encore numéro de série), Workspace ONE UEM utilise ces attributs pour faire correspondre automatiquement un terminal enrôlé avec son enregistrement.

Lorsque des informations d'enregistrement inadéquates sont fournies, le niveau de priorité suivant permet à Workspace ONE UEM d'inscrire des terminaux avec succès.

1 Utilisateur pour lequel le terminal est enregistré.

2 Plateforme (si elle est indiquée).

3 Modèle (s'il est indiqué).

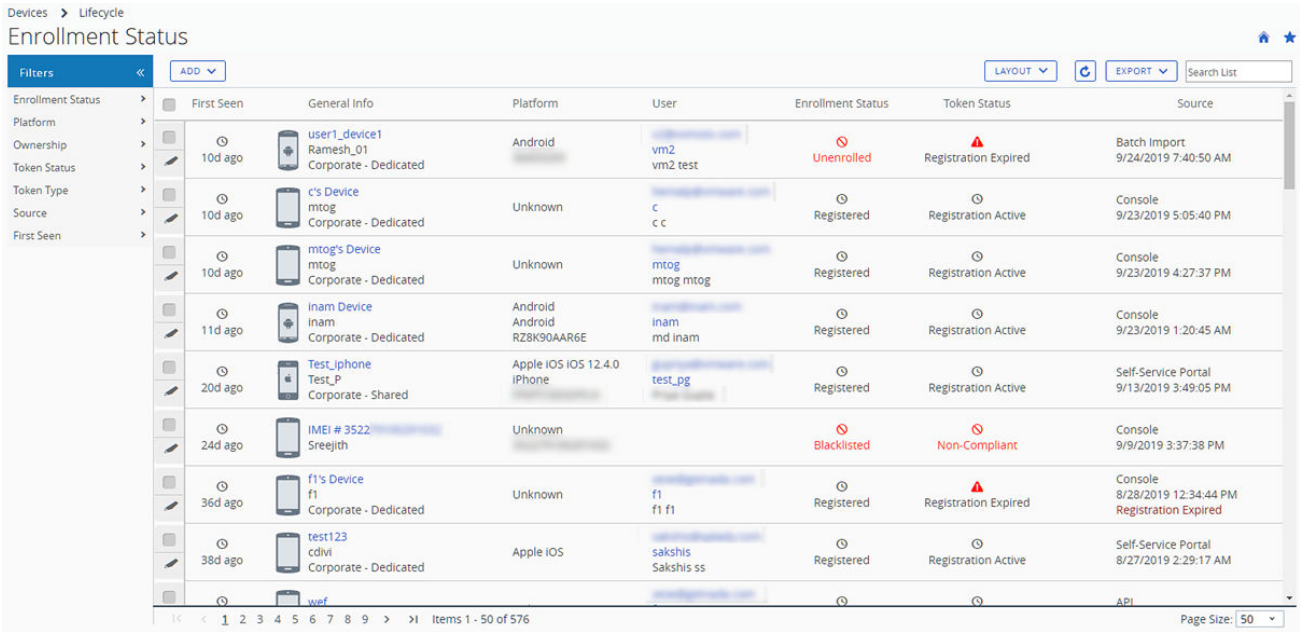
4 Type de propriété (s'il est indiqué).

5 Date de la plus ancienne inscription correspondante.

État de l'enrôlement

Vous pouvez évaluer l'état d'enrôlement par terminal dans Workspace ONE UEM powered by AirWatch, importer et enrôler en masse des terminaux, mettre des terminaux sur liste autorisée/bloquée et révoquer/réinitialiser les jetons des terminaux en consultant le statut d'enrôlement.

Cliquez sur **Terminaux > Cycle de vie > Statut d'enrôlement** pour afficher une liste complète de tous les terminaux par statut d'enrôlement au niveau du groupe organisationnel sélectionné.



Triez par colonne et configurez les filtres d'informations pour vérifier les activités du terminal selon des informations précises. Par exemple, triez la colonne **Statut du jeton** pour n'afficher que les terminaux dont l'inscription n'est pas applicable et agir uniquement sur ces terminaux spécifiques. Effectuez une recherche parmi les terminaux par nom convivial ou nom d'utilisateur pour isoler un terminal ou un utilisateur.

Paramètre	Description
Filtres	Vous pouvez exclure des catégories de terminaux complètes à l'aide de filtres afin de ne voir que les terminaux qui vous intéressent. ■ **Statut d'enrôlement** ■ **Plateforme** ■ **Propriété** ■ **Statut du jeton** ■ **Type de jeton** ■ **Source** ■ **Première connexion**
Bouton **Ajouter**	■ **Inscrire un terminal** – Vous pouvez inscrire ou **ajouter** un seul terminal à enrôler. ■ **Mettre les terminaux sur liste bloquée ou autorisée** – Vous pouvez autoriser l'enrôlement de terminaux identifiés ou mis sur liste autorisée seulement. Sinon, vous pouvez empêcher l'enrôlement de terminaux en les mettant sur liste bloquée. ■ **Importation par lot** – Importez plusieurs terminaux ou plusieurs utilisateurs avec l'écran Importation par lots.
Renvoyer le message	Renvoyez simplement le message original à l'utilisateur, avec l'URL du portail en libre-service, l'ID de groupe et les identifiants de connexion.
Plus d'actions	
Modifier le groupe organisationnel	Déplacez le terminal sélectionné vers le groupe organisationnel de votre choix.
Modifier le type de propriété	Modifiez le type de propriété du terminal sélectionné.
Supprimer	Supprimez définitivement les informations des terminaux sélectionnés. Cette action oblige l'utilisateur à se réinscrire pour s'enrôler. Le cas échéant, vous devez d'abord annuler le jeton avant la suppression de l'inscription d'un terminal.
Réinitialiser le jeton	Réinitialisez le statut du jeton s'il a été annulé ou s'il a expiré.
Annuler le jeton	Forcez l'expiration du statut du jeton d'inscription des terminaux sélectionnés, en bloquant l'accès pour les utilisateurs ou terminaux non désirés. Pour les actions **Réinitialiser le jeton** et **Révoquer le jeton**, vous pouvez choisir de désactiver le paramètre **Notifier les utilisateurs** qui empêche l'envoi de la notification par e-mail par défaut.
Sélection de plusieurs terminaux	Effectuez des actions sur un ou plusieurs terminaux en le/les cochant et en utilisant les boutons d'action. Après avoir appliqué un filtre pour afficher un ensemble spécifique de terminaux, vous pouvez effectuer des actions en masse sur de nombreux terminaux sélectionnés. Effectuez cette opération en sélectionnant les terminaux, puis en choisissant une action des boutons **Renvoyer le message** et **Plus d'actions**. Vous pouvez cocher les différentes cases. Vous pouvez également sélectionner l'ensemble des terminaux filtrés en cochant la case principale située au-dessus de la colonne. Lorsque vous sélectionnez une action pour un ou plusieurs terminaux, un écran de confirmation apparaît vous permettant d'**enregistrer** ou d'**annuler** l'action.

Paramètre	Description
Bouton **Affichage**	Affichez la liste complète des colonnes visibles ou choisissez d'afficher ou de masquer les colonnes selon vos préférences en sélectionnant l'option **Personnalisée**. Vous pouvez aussi appliquer vos colonnes personnalisées à tous les administrateurs au niveau du groupe organisationnel actuel ou en dessous de celui-ci. Vous pouvez revenir aux paramètres du bouton **Mise en page** à tout moment pour modifier vos préférences d'affichage de la colonne.
Bouton **Exporter**	Vous pouvez télécharger des rapports de l'affichage en liste **État de l'enrôlement**, au format Excel par défaut (**.xlsx**), ou au format **.csv** (valeurs séparées de virgules).

Depuis l'**affichage des détails**, vous pouvez renvoyer le message d'enrôlement en cliquant sur bouton **Renvoyer le message**. Vous pouvez également modifier les informations d'inscription d'un terminal en cliquant sur le bouton **Modifier l'inscription** et en remplissant la section **Informations avancées sur le terminal**.

L'**affichage des détails** présente une série d'onglets, chacun contenant des informations d'enrôlement relatives au terminal.

- **Résumé** – Affichez la date d'inscription, le temps écoulé depuis la dernière connexion du terminal et des informations basiques sur le terminal et l'utilisateur.
- **Utilisateur** – Affichez les détails de l'utilisateur.
- **Message** – Affichez l'e-mail d'envoi relatif à l'activation du terminal, dont les identifiants et le code QR. Il existe une option « Message d'inscription de l'utilisateur » qui permet à l'administrateur de masquer l'onglet **Message** après un enrôlement réussi du terminal.
- **Attributs personnalisés** – Affichez les attributs personnalisés associés au terminal.
- **Étiquettes** – Affichez les étiquettes associées au terminal.
- **Enrôlement hors ligne** – Si cette option est disponible, elle vous permet d'enrôler votre terminal hors ligne. Cette fonctionnalité est utile lorsque vous souhaitez utiliser le terminal hors ligne (par exemple, lors de vos déplacements).

Auto-enrôlement ou préenrôlement

Workspace ONE UEM propose deux méthodes d'enrôlement des terminaux professionnels. Vous pouvez laisser vos utilisateurs enrôler leurs propres terminaux ou les administrateurs peuvent le faire à leur place dans le cadre d'un processus appelé **pré-enrôlement du terminal**.

Lors du préenrôlement des terminaux, l'administrateur enrôle les terminaux avant de les attribuer et de les distribuer aux utilisateurs. Cette méthode est utile pour les administrateurs qui doivent configurer des terminaux pour les utilisateurs finaux au sein d'une organisation.

Le préenrôlement peut être réalisé sur les terminaux Android, iOS et macOS.

Considération 1 : propriété des terminaux

- Vos utilisateurs ont-ils déjà des terminaux professionnels attribués ? Si c'est le cas, il est plus pratique d'autoriser les utilisateurs à procéder eux-mêmes à l'enrôlement plutôt que de collecter chaque terminal pour le préenrôler.
- Vos utilisateurs partagent-ils les terminaux ou utilisent-ils leurs propres appareils ? S'ils ne partagent pas les terminaux, vous pouvez alors confier la responsabilité de l'inscription de ceux -ci à chaque utilisateur.

  Le préenrôlement des terminaux fonctionne également parfaitement pour les terminaux provisionnés puisqu'il est effectué avant que l'employé ne reçoive le terminal. Si vos utilisateurs ont déjà des terminaux d'entreprise, il est conseillé de les autoriser à s'auto-enrôler. Le fait de laisser les utilisateurs enrôler leurs propres terminaux est également intéressant lorsque le nombre total de terminaux ne permet pas aux administrateurs d'effectuer leur préenrôlement.

Considération 2 : détection automatique

Associez-vous votre domaine de messagerie d'entreprise à l'environnement Workspace ONE UEM ? Ce processus, connu sous le nom de **détection automatique**, signifie que les utilisateurs n'ont besoin que de leur adresse e-mail et de leurs identifiants. L'URL d'enrôlement et l'ID de groupe sont entrés automatiquement.

Consultez également la rubrique Enrôlement par détection automatique.

Considération 3 : enrôlement direct de Workspace ONE

Le préenrôlement de terminal via l'enrôlement direct de Workspace ONE n'est pas pris en charge. Si vous devez préenrôler un terminal pour un ou plusieurs utilisateurs, vous devez enrôler le terminal à l'aide de Workspace ONE Intelligent Hub au lieu d'utiliser l'enrôlement direct de Workspace ONE.

L'enrôlement direct de Workspace ONE est une fonction qui convient parfaitement à l'auto-enrôlement. Une fois activés, tous les terminaux qualifiés qui se connectent au groupe organisationnel d'enrôlement sont immédiatement enrôlés. Une fois l'installation terminée, l'utilisateur final peut accepter d'installer les applications sélectionnées par l'entreprise ou refuser leur installation.

Pour plus d'informations, consultez la section Enrôlement direct de Workspace ONE.

Considération 4 : participez-vous au programme d'enrôlement des terminaux Apple ?

Pour tirer le meilleur parti des terminaux Apple enrôlés dans le MDM, Apple a mis en place le programme d'inscription des appareils Apple (Device Enrollment Program, aussi appelé DEP). Grâce à DEP, vous pouvez réaliser les actions suivantes.

- Installer un profil MDM non supprimable afin d'empêcher les utilisateurs finaux de l'effacer.

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

Considération 5 : utilisation d'Apple Configurator

Apple Configurator permet aux administrateurs de déployer et gérer efficacement les terminaux iOS. Les organisations telles que les magasins, les écoles ou les hôpitaux trouveront cette fonctionnalité particulièrement utile pour préenrôler des terminaux afin qu'ils soient partagés par plusieurs utilisateurs.

L'utilisation d'Apple Configurator pour enrôler des terminaux pré-inscrits et destinés à un seul utilisateur est prise en charge en ajoutant le numéro de série/l'IMEI à un terminal inscrit dans la console AirWatch. L'un des principaux avantages d'Apple Configurator est l'utilisation d'un hub USB ou d'un chariot de terminal pour provisionner plusieurs terminaux en quelques minutes.

Considération 6 : préenrôlement d'un utilisateur unique ou inscription ?

Si vous envisagez de préenrôler des terminaux pour un utilisateur unique, il serait préférable de procéder à une inscription. La différence entre le préenrôlement pour un utilisateur unique et l'inscription d'un terminal est subtile, mais importante.

Inscription – Lorsque vous inscrivez un terminal, vous le faites pour un utilisateur identifié unique. Cette procédure signifie que le terminal s'attend à ce que le premier utilisateur à se connecter soit l'utilisateur pour lequel il a été enregistré. Si un autre utilisateur tente de se connecter à un terminal inscrit, le terminal est verrouillé pour des raisons de sécurité et il ne peut pas être enrôlé.

Préenrôlement d'un utilisateur unique – Lorsque vous préenrôlez un terminal, vous le faites pour tous les utilisateurs qualifiés pour s'enrôler dans Workspace ONE UEM. En théorie, vous pourriez remettre un terminal préenrôlé à n'importe quel utilisateur qualifié, qui pourrait alors se connecter au terminal et s'enrôler dans Workspace ONE UEM.

Le processus de préenrôlement vous permet de préparer le terminal et de démarrer Workspace ONE Intelligent Hub, auquel n'importe quel utilisateur qualifié peut se connecter. Workspace ONE UEM effectue ensuite une réattribution ponctuelle pour associer le terminal à cet utilisateur.

Considération 7 : utilisation du préenrôlement de terminaux

Sauf si vous utilisez Apple Configurator, les administrateurs doivent préenrôler les terminaux les uns après les autres. Pour les déploiements de grande taille, prenez en compte le temps et le personnel nécessaires.

Si les administrateurs peuvent préenrôler facilement les nouveaux terminaux, les employés qui utilisent déjà des terminaux appartenant à l'entreprise doivent envoyer et récupérer leurs terminaux pour qu'ils soient préenrôlés.

Si vous avez des milliers de terminaux à préenrôler, le préenrôlement peut prendre du temps. Ainsi, cette méthode fonctionne mieux si vous avez un nouveau lot de terminaux en arrivage, puisque vous avez accès aux terminaux avant que les employés ne les reçoivent.

Le préenrôlement peut être réalisé sur les terminaux Android et iOS de plusieurs façons :

- **Utilisateur unique (standard)** – S'utilise lorsque vous préenrôlez un terminal que n'importe quel utilisateur peut enrôler.

  Note Comme indiqué, ce flux d'enrôlement est destiné aux terminaux sans surveillance. Si vous utilisez ce flux pour l'enrôlement de l'utilisateur sans contact, vous êtes tenu de vous assurer que les terminaux préenrôlés sont fournis à l'utilisateur prévu.

- **Utilisateur unique (avancé)** – Permet le préenrôlement et l'enrôlement d'un terminal pour un utilisateur spécifique.

  Note L'utilisateur ou l'administrateur intermédiaire doit s'assurer que le terminal est extrait par l'utilisateur enregistré.

- **Utilisateurs multiples** – Permet le préenrôlement d'un terminal qui sera partagé par plusieurs utilisateurs.

  Pour obtenir des instructions détaillées, consultez la rubrique Créer un compte de préenrôlement multi-utilisateurs pour l'enrôlement.

Préenrôler des terminaux à utilisateur unique

Utile pour les administrateurs informatiques déployant une flotte de terminaux, le préenrôlement de terminaux à utilisateur unique de Workspace ONE UEM Console permet à un seul administrateur de provisionner les terminaux à la place des utilisateurs.

Le préenrôlement de terminal via l'enrôlement direct de Workspace ONE n'est pas pris en charge. Si vous devez préenrôler un terminal pour un ou plusieurs utilisateurs, vous devez enrôler le terminal à l'aide de Workspace ONE Intelligent Hub au lieu d'utiliser l'enrôlement direct de Workspace ONE.

Important La possibilité de créer des utilisateurs préenrôlés est un privilège d'administrateur de niveau élevé. Seuls les administrateurs approuvés spécifiques devraient être autorisés à créer un utilisateur préenrôlé. Vous devez également traiter les informations d'identification de l'utilisateur préenrôlé comme vous le feriez pour tout autre privilège d'administrateur. En outre, ne divulguez pas les informations d'identification de l'utilisateur.

Actuellement, tout administrateur autorisé à créer un utilisateur peut également créer un utilisateur préenrôlé. Limitez cette possibilité en modifiant les rôles attribués à vos administrateurs. Accédez à**Comptes > Administrateurs > Rôles**. Identifiez uniquement les rôles que vous souhaitez limiter, puis cliquez sur **Modifier** ( ) pour modifier chacun de ces rôles dans le chemin de catégorie**Tous les > comptes > Comptes > utilisateurs**en décochant la case **Modifier** de l'autorisation « Ajouter/Modifier ».

Note Une liaison LDAP est requise pour le préenrôlement de terminaux. Pour créer cette section de configuration, consultez la section Lier un terminal au service d'annuaire dans ce guide.

1 Accédez à **Comptes > Utilisateurs > Affichage en liste** et sélectionnez **Modifier** pour le compte utilisateur pour lequel vous souhaitez activer le préenrôlement.

2 Sur la page **Ajouter/Modifier un utilisateur**, cliquez sur l'onglet **Avancé**.

   a Faites défiler vers le bas jusqu'à la section **Préenrôlement**.

   b Pour l'option **Activer le préenrôlement de terminaux**, positionnez le curseur sur **Activé**. Les options de préenrôlement s'affichent.

   c Pour l'option **Terminaux à utilisateur unique**, positionnez le curseur sur **Activé**.

   d Sélectionnez le type de mode de préenrôlement de terminal à utilisateur unique en choisissant **Standard** ou **Avancé**.

   Avec le préenrôlement standard, un utilisateur final devra entrer ses informations de connexion après le préenrôlement, tandis qu'en mode Avancé, l'utilisateur du préenrôlement enrôle le terminal pour un autre utilisateur.

   e Assurez-vous que l'option **Terminaux partagés** est **désactivée**.

   f Sous l'option **Mode Terminaux partagés Android**, sélectionnez **Natif** ou **Launcher** pour les modes check-in et check-out. Android natif prend en charge des cas d'utilisation plus simples qui ne nécessitent pas de personnalisation. Launcher prend en charge la personnalisation de l'interface utilisateur pour les cas d'utilisation complexes.

   g Sous **Applications système**, vous pouvez activer l'accès de l'utilisateur aux applications système.

h Sous **Code secret du mode administrateur**, spécifiez un code d'accès alphanumérique pour dépanner un terminal en mode administrateur. Appuyez 5 fois sur l'icône Hub de l'écran de connexion pour accéder au mode administrateur.

Résultat : l'option **Terminaux à utilisateur unique** préenrôle les terminaux pour un utilisateur unique.

3 Enrôler le terminal. Les choix sont les suivants :

- Enrôlez le terminal à l'aide de Workspace ONE Intelligent Hub en saisissant une URL de serveur et un ID de groupe.
- Ouvrez le navigateur Internet du terminal, naviguez vers l'URL d'enrôlement et saisissez l'ID de groupe.

4 Saisissez vos identifiants d'utilisateur de préenrôlement lors de l'enrôlement.

a Le cas échéant, indiquez que le préenrôlement concerne un **terminal à utilisateur unique**.

Vous n'aurez à indiquer cela que si le préenrôlement de terminaux partagés est également activé.

5 Terminez le préenrôlement avancé ou standard.

a En cas de préenrôlement avancé, vous devez saisir le nom d'utilisateur de la personne qui utilisera le terminal. Poursuivez l'enrôlement en installant le profil MDM et en acceptant l'ensemble des invites et des messages.

b Dans le cas d'un préenrôlement standard, à la fin de celui-ci il est demandé à l'utilisateur final de saisir ses identifiants dans la fenêtre de connexion.

Résultat : le préenrôlement du terminal est maintenant terminé ; il est prêt à être utilisé par le nouvel utilisateur. Si un contrat des conditions d'utilisation de l'inscription est en place, l'utilisateur unique préenrôlé ne verra pas cette invitation à accepter les CGU jusqu'à ce qu'il se connecte à son compte SSP.

Préenrôler des terminaux partagés

Le préenrôlement de terminaux partagés permet à un administrateur informatique de configurer des terminaux qui seront ensuite utilisés par plusieurs utilisateurs. Le préenrôlement de plusieurs utilisateurs permet au terminal de modifier dynamiquement son utilisateur attribué selon que différents utilisateurs du réseau se connectent à ce terminal.

Le préenrôlement de terminal via l'enrôlement direct de Workspace ONE n'est pas pris en charge. Si vous devez préenrôler un terminal pour un ou plusieurs utilisateurs, vous devez enrôler le terminal à l'aide de Workspace ONE Intelligent Hub au lieu d'utiliser l'enrôlement direct de Workspace ONE.

1 Accédez à **Comptes > Utilisateurs > Affichage en liste** et sélectionnez **Modifier** pour le compte utilisateur pour lequel vous souhaitez activer le préenrôlement.

2 Sur la page **Ajouter/Modifier un utilisateur**, cliquez sur l'onglet **Avancé**.

a Faites défiler vers le bas jusqu'à la section **Préenrôlement**.

b Pour l'option **Activer le préenrôlement de terminaux**, positionnez le curseur sur **Activé**. Les options de préenrôlement s'affichent.

c Assurez-vous que l'option **Terminaux partagés** est **activée**.

d Sous l'option **Mode Terminaux partagés Android**, sélectionnez **Natif** ou **Launcher** pour les modes check-in et check-out. Android natif prend en charge des cas d'utilisation plus simples qui ne nécessitent pas de personnalisation. Launcher prend en charge la personnalisation de l'interface utilisateur pour les cas d'utilisation complexes.

e Sous **Applications système**, vous pouvez activer l'accès de l'utilisateur aux applications système.

f Sous **Code secret du mode administrateur**, spécifiez un code d'accès alphanumérique pour dépanner un terminal en mode administrateur. Appuyez 5 fois sur l'icône Hub de l'écran de connexion pour accéder au mode administrateur.

3 Enrôlez le terminal en suivant l'une des deux méthodes suivantes.

- Enrôlez le terminal à l'aide de Workspace ONE Intelligent Hub en saisissant une URL de serveur et un ID de groupe.
- Ouvrez le navigateur Internet du terminal, naviguez vers l'URL d'enrôlement et saisissez l'ID de groupe.

4 Saisissez vos identifiants d'utilisateur de préenrôlement lors de l'enrôlement. Le cas échéant, indiquez que le préenrôlement concerne un **terminal à utilisateur unique**.

Vous ne devez le faire que si le préenrôlement de terminaux partagé est également activé.

Résultat : le préenrôlement du terminal est maintenant terminé ; il est prêt à être utilisé par les nouveaux utilisateurs.

Processus d'auto-enrôlement

L'auto-enrôlement peut nécessiter que les utilisateurs connaissent leur ID de groupe et leurs identifiants de connexion. Si vous avez intégré les services d'annuaire, ces identifiants sont les mêmes que ceux des services d'annuaire.

Vous pouvez aussi associer votre domaine de messagerie d'entreprise avec l'environnement Workspace ONE UEM dans le cadre d'un processus appelé détection automatique. Lorsque l'option de détection automatique est activée, les terminaux des plateformes prises en charge invitent les utilisateurs à saisir leur adresse e-mail. Ces terminaux effectuent l'enrôlement automatiquement si leur domaine de messagerie (la partie à droite du caractère @) correspond, sans qu'ils aient besoin d'entrer un ID de groupe ou une URL d'enrôlement. Pour plus d'informations, consultez la section Enrôlement par détection automatique.

1 Les utilisateurs accèdent à AWAgent.com qui détecte automatiquement si Workspace ONE Intelligent Hub est installé.

Si Workspace ONE Intelligent Hub n'est pas installé, le site Web les redirige vers l'app store mobile approprié.

2 Les utilisateurs d'AirWatch Container téléchargent l'application AirWatch Container depuis le magasin d'applications.

3 Après avoir lancé Workspace ONE Intelligent Hub ou l'application Container, les utilisateurs saisissent leurs identifiants, en plus de leur adresse e-mail ou de l'URL/ID de groupe, et poursuivent l'enrôlement.

Mode supervisé

Les administrateurs ont la possibilité d'activer le mode supervisé pour les terminaux enrôlés via Apple Configurator, permettant ainsi d'utiliser davantage de fonctionnalités de sécurité avancées. Cependant, ce mode entraîne certaines limites sur le terminal.

Avantages

Une fois le terminal supervisé et enrôlé dans Workspace ONE UEM, l'administrateur dispose des fonctionnalités avancées de configuration suivantes en comparaison des terminaux classiques.

- **Restrictions élevées sur le MDM**
  - Empêchez les utilisateurs de supprimer les applications. La suppression d'applications peut aussi être limitée localement sur le terminal à l'aide des restrictions dans la section Configuration du système.
  - Interdisez AirDrop.
  - Empêchez les utilisateurs de modifier les paramètres du compte de messagerie et d'iCloud afin d'éviter toute modification du compte.
  - Désactivez iMessage.
  - Définissez les restrictions de notations du contenu dans l'iBookstore.
  - Désactivez Game Center et iBookstore.
- **Sécurité avancée**
  - Empêchez les utilisateurs de consulter des sites pour adultes dans Safari.
  - Déterminez quels terminaux peuvent se connecter aux destinations spécifiées d'AirPlay, telles qu'Apple TVs.
  - Empêchez l'installation de profils de configuration non gérés ou de certificats.
  - Forcez tout le trafic réseau à travers un proxy HTTP global.
- **Mode Kiosque**
  - Verrouillez les terminaux sur une application grâce au mode Application unique et désactivez le bouton d'accueil.
- **Personnaliser le papier peint et le texte sur le terminal**
- **Activer ou effacer le verrou d'activation**

Limites

- L'accès USB aux terminaux supervisés est limité au Mac de surveillance.

- Impossible de copier des données vers et depuis le terminal à l'aide d'iTunes, à moins que le certificat d'identité Apple Configurator ne soit installé sur le terminal.
    - Les médias tels que les photos et les vidéos ne peuvent pas être copiés depuis le terminal sur un PC ou un Mac. Pour transférer ce type de données, utilisez VMware Content Locker pour synchroniser le contenu avec la section Documents personnels de l'utilisateur. Vous pouvez sinon utiliser une application de partage de fichiers pour transférer les données par WLAN/WWAN sur un serveur.
- Le mode supervisé empêche l'accès aux journaux depuis les terminaux avec iPhone Configuration Utility (IPCU).
    - Ce mode complique la résolution des problèmes d'applications ou de terminaux. Les journaux des terminaux ne peuvent en effet s'obtenir que si le terminal est connecté au Mac qui le supervise. Pour relever certains défis, utilisez Workspace ONE SDK pour envoyer les journaux, des applications à UEM Console.
- Les terminaux ne peuvent pas être réinitialisés avec les paramètres d'usine facilement.
    - Une fois le terminal réinitialisé aux paramètres d'usine, il doit être rapporté au Mac de surveillance pour rétablir le mode supervisé. Cette procédure peut être problématique si le Mac ne se trouve pas près du terminal.

Pour décider si oui ou non vous devez activer le mode supervisé, prenez en compte les éléments suivants. Malgré l'activation de fonctions de sécurité supplémentaires sur le terminal, vous devez considérer les limites USB.

La proximité entre le terminal et le Mac de surveillance est déterminante dans la prise de décision. Étant donné que les limites de l'USB empêchent l'accès aux journaux du côté du terminal, si un appareil rencontre des problèmes, il doit être renvoyé dans un dépôt et à nouveau préenrôlé pour restaurer les fonctionnalités.

Le choix de superviser ou de ne pas superviser à l'avance les terminaux est important, car ce processus obligera l'envoi des appareils vers un dépôt ou des bureaux informatiques.

Ordre de priorité des groupes organisationnels pour l'enrôlement des utilisateurs

Le groupe organisationnel qui devient le groupe organisationnel d'enrôlement d'un utilisateur joue un rôle spécial dans la gestion des terminaux et des utilisateurs. Une hiérarchie de sélection détermine le groupe organisationnel qui devient le groupe organisationnel d'enrôlement d'un utilisateur.

Le groupe organisationnel utilisé comme groupe organisationnel d'enrôlement d'un utilisateur est sélectionné en fonction de l'ordre de priorité suivant.

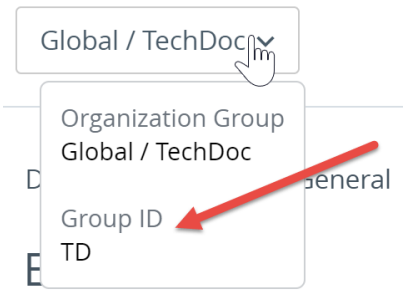
1. GROUPE ORGANISATIONNEL DU GROUPE D'UTILISATEURS AUQUEL L'UTILISATEUR APPARTIENT

- Configurez cette option en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et, dans l'onglet **Regroupement**, sélectionnez **Sélectionner automatiquement en fonction du groupe d'utilisateurs** comme **Mode d'attribution de l'ID de groupe**. Pour plus d'informations, reportez-vous à Configurer les options d'enrôlement dans l'onglet Regroupement.

Si la sélection ci-dessus n'est pas effectuée ou si l'utilisateur ne fait pas partie d'un groupe d'utilisateurs, le groupe organisationnel d'enrôlement devient le...

2. GROUPE ORGANISATIONNEL FOURNI LORS DE L'ENRÔLEMENT

- Configurez cette option en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et, dans l'onglet **Regroupement**, sélectionnez **Par défaut** comme **Mode d'attribution de l'ID de groupe**.
  - Vous devez ensuite fournir le nom de l'ID de groupe que l'utilisateur doit entrer au moment de l'enrôlement. En général, il est communiqué aux utilisateurs dans un e-mail qui contient une URL d'enrôlement.
  - Vous pouvez obtenir l'ID de groupe du groupe organisationnel dans lequel vous vous trouvez en survolant à l'aide du pointeur de la souris le sélecteur de groupe organisationnel et en consultant la fenêtre contextuelle qui s'affiche.



- Vous pouvez également laisser l'utilisateur effectuer une sélection dans une liste d'ID de groupe. Activez cette option en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et, dans l'onglet **Regroupement**, sélectionnez **Sélection manuelle de l'ID de groupe par l'utilisateur** comme **Mode d'attribution de l'ID de groupe**.
  - Au moment de l'enrôlement, une liste de groupes organisationnels enfants (appartenant au groupe organisationnel parent dans lequel vous vous trouvez) s'affiche, dans laquelle l'utilisateur peut sélectionner son ID de groupe (groupe organisationnel d'enrôlement). Cette option ne vous oblige pas à effectuer un mappage d'attribution de groupe et les utilisateurs ont la liberté de sélectionner un groupe organisationnel enfant dans la liste.

Si l'ID de groupe n'est pas communiqué à l'utilisateur avant l'enrôlement et que l'utilisateur ne fait pas partie d'un groupe d'utilisateurs, le groupe organisationnel d'enrôlement devient le...

3. GROUPE ORGANISATIONNEL BASÉ SUR L'ID DU GROUPE DE DÉTECTION AUTOMATIQUE

- Configurez cette option en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et, dans l'onglet **Authentification**, ajoutez un domaine de messagerie correspondant à l'adresse e-mail professionnelle de l'utilisateur. Pour plus d'informations sur l'onglet **Authentification**, reportez-vous à Configurer les options d'enrôlement.
    - Au moment de l'enrôlement, l'utilisateur est invité à saisir son adresse e-mail professionnelle. Le terminal de l'utilisateur est automatiquement enrôlé dans le groupe organisationnel approprié en fonction du domaine de l'adresse e-mail saisie.

Si aucune des options ci-dessus n'est configurée, le groupe organisationnel d'enrôlement devient le...

4. GROUPE ORGANISATIONNEL SÉLECTIONNÉ LORS DE L'AJOUT DE L'UTILISATEUR

- Configurez cette option lorsque vous ajoutez des utilisateurs dans la Workspace ONE UEM Console en accédant à **Comptes > Utilisateurs > Affichage en liste** et sélectionnez **Ajouter** suivi de **Ajouter un utilisateur**. Dans l'écran **Ajouter/modifier un utilisateur** qui s'affiche, faites défiler la liste vers le bas et ouvrez la section **Enrôlement**. Complétez l'option **Groupe organisationnel d'enrôlement**.
- Sinon, si vous ne sélectionnez aucun groupe organisationnel dans la section **Enrôlement** de l'écran **Ajouter/Modifier un utilisateur**, le groupe organisationnel d'enrôlement de l'utilisateur devient le groupe organisationnel dans lequel vous vous trouvez au moment où vous ajoutez l'utilisateur.

Enrôlement direct de Workspace ONE

L'enrôlement direct dans Workspace ONE UEM vous permet d'enrôler vos terminaux de la manière la plus rapide possible.

L'enrôlement direct représente la manière la plus régulière d'enrôler des terminaux qui appartiennent à l'entreprise et qui sont personnellement activés (COPE). Le modèle COPE permet aux entreprises de trouver un équilibre entre la consumérisation des terminaux et la sécurité et le contrôle requis.

En tant qu'administrateur, vous pouvez configurer l'enrôlement direct avec les options de votre choix. Vous pouvez configurer une invite facultative, appliquer des restrictions par type de terminal ou des limites par groupe d'utilisateurs, et permettre à l'utilisateur d'installer les applications.

Activation de l'enrôlement direct pour Workspace ONE

Vous pouvez activer l'enrôlement direct de Workspace ONE™ dans le groupe organisationnel (OG) de votre choix. Une fois activé, tous les terminaux qualifiés qui se connectent pour la première fois à Workspace ONE UEM sont directement enrôlés. Les terminaux non qualifiés qui ne répondent pas aux critères que vous définissez sont enrôlés à un état conteneur ou non géré.

L'enrôlement direct est désactivé par défaut. Pour activer l'enrôlement direct de Workspace ONE, procédez comme suit.

1 Basculez vers le groupe organisationnel pour lequel vous souhaitez activer l'enrôlement direct de Workspace ONE.

2 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et sélectionnez l'onglet **Restriction**.

3 Si nécessaire, sélectionnez Remplacer pour remplacer les paramètres du groupe organisationnel parent.

4 Faites défiler vers le bas jusqu'à la section **Conditions de gestion pour Workspace ONE** et sélectionnez vos options de configuration.

Paramètre	Description
MDM requis pour Workspace ONE	Invitez les terminaux et les utilisateurs qualifiés à s'enrôler immédiatement après s'être connectés à Workspace ONE. Les terminaux en dehors des critères définis sont autorisés à s'enrôler à un état non géré et peuvent être gérés ultérieurement (gestion adaptative).
Groupe d'utilisateurs affecté	Ce paramètre spécifie le groupe d'utilisateurs que vous souhaitez inclure dans le processus d'enrôlement direct. Vous pouvez également choisir l'option **Tous les utilisateurs** qui correspond à la sélection par défaut lorsque vous activez **MDM requis pour Workspace ONE**.
iOS	Activez ce paramètre pour inclure les terminaux iOS. Si cette option est désactivée, les terminaux iOS ne sont pas éligibles à l'enrôlement direct, mais ils peuvent toujours s'enrôler dans Workspace ONE UEM à un état non géré.
Android hérité	Activez cette option pour inclure les terminaux Android hérités. Si cette option est désactivée, les terminaux Android hérités ne sont pas éligibles à l'enrôlement direct, mais ils peuvent toujours s'enrôler dans Workspace ONE UEM à un état non géré.
Android Enterprise	Activez ce paramètre pour inclure les terminaux Android Enterprise. Si cette option est désactivée, les terminaux Android Enterprise ne sont pas éligibles à l'enrôlement direct, mais ils peuvent toujours s'enrôler dans Workspace ONE UEM à un état non géré.

Résultat : seules les options prises en charge configurées dans les autres onglets d'enrôlement s'appliquent à votre configuration d'enrôlement direct enregistrée.

Que faire ensuite ? Après avoir activé l'enrôlement direct de Workspace ONE, vous pouvez ensuite **enrôler votre terminal avec l'enrôlement direct de Workspace ONE**. Pour plus d'informations sur les options de l'enrôlement direct de Workspace ONE et sur les options d'enrôlement en général, consultez les autres sections sur cette page.

Enrôler votre terminal avec l'enrôlement direct de Workspace ONE

Si l'enrôlement direct de Workspace ONE™ est activé, lorsque vous vous connectez au groupe organisationnel d'enrôlement à l'aide d'un terminal et d'un utilisateur qualifiés avec l'application Workspace ONE, cela signifie que vous êtes immédiatement enrôlé.

Vos utilisateurs ont également la possibilité d'installer immédiatement les applications que votre entreprise trouve utiles. Vous pouvez également ignorer cette étape et installer l'application ultérieurement. Pour enrôler un terminal avec l'enrôlement direct de Workspace ONE, l'utilisateur doit procéder comme suit.

1 Télécharger, installer et exécuter l'application Workspace ONE depuis le référentiel ou le magasin d'applications de la plateforme.

2 Entrer l'adresse e-mail ou l'URL du serveur.

3 Entrer son nom d'utilisateur et son mot de passe pour les services d'annuaire.

4 Installer ou activer **Workspace Services** en sélectionnant les étapes positives propres à la plateforme utilisée.

   a **iOS** – Autoriser le serveur à ouvrir les **Paramètres**, entrer le code d'accès du terminal, installer un profil de terminal non signé et ouvrir un écran dans Workspace.

   b **Android hérité** – Installer Workspace ONE Intelligent Hub, lui permettre de passer et de gérer les appels téléphoniques, sélectionner le propriétaire de son terminal avec une option pour entrer le numéro d'actif du terminal, activer l'application d'administration du terminal, puis se connecter à Workspace ONE.

   c **Android Enterprise** – Accepter (ou refuser) les conditions d'utilisation, établir le profil de travail et créer le code d'accès Workspace ONE.

5 Lorsque Workspace ONE termine la routine d'installation, vous pouvez **continuer à installer des applications**.

6 Vous pouvez installer les applications une par une en les sélectionnant dans une liste, **toutes les installer** ou **ignorer** complètement cette étape.

Options prises en charge par l'enrôlement direct de Workspace ONE

La fonctionnalité Enrôlement direct de Workspace ONE fonctionne avec la plupart des options d'enrôlement existantes et des plateformes disponibles avant le développement de la fonctionnalité.

L'enrôlement direct avec Workspace ONE™ prend en charge les plateformes et les options d'enrôlement suivantes.

Plateformes prises en charge

- iOS.
- Android hérité.

- Android Enterprise.

Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement**, sélectionnez chaque onglet applicable et effectuez vos sélections en fonction de la compatibilité avec l'enrôlement direct de Workspace ONE.

Authentification

Les options d'authentification suivantes sont compatibles avec l'enrôlement direct de Workspace ONE.

- Utilisateurs des services d'annuaire.
- Les utilisateurs SAML plus Active Directory sont pris en charge « à la volée ». Les utilisateurs SAML sans LDAP sont pris en charge tant que l'enregistrement de l'utilisateur préexiste dans Workspace ONE UEM au moment de la connexion initiale.

  Les utilisateurs basiques, préenrôlés, SAML sans annuaire et Proxy d'authentification ne sont pas pris en charge actuellement.
- Enrôlement ouvert.
- Workspace ONE n'audite pas les paramètres Exiger l'enrôlement par Workspace ONE Intelligent Hub pour les terminaux iOS ou macOS qui sont utilisés pour bloquer l'enrôlement Web sur leurs plateformes respectives.

Conditions d'utilisation

Toutes les options des conditions d'utilisation sont compatibles avec l'enrôlement direct de Workspace ONE.

Regroupement

Toutes les options de regroupement sont compatibles avec l'enrôlement direct de Workspace ONE.

Restrictions

Les options des restrictions suivantes sont compatibles avec l'enrôlement direct de Workspace ONE.

- Utilisateurs connus et groupes configurés.
- Limite du nombre maximal de terminaux enrôlés.
- Les paramètres de la politique sont partiellement pris en charge.
  - Types de propriété autorisés – Workspace ONE affiche une invite uniquement pour les terminaux personnels et professionnels. Pour éviter cela, désactivez l'invite facultative et utilisez le type de propriété par défaut.
  - Les types d'enrôlement autorisés ne sont pas pris en charge.

- Les restrictions relatives au système d'exploitation, au modèle et à la plateforme du terminal sont prises en charge.
- Restrictions de groupe d'utilisateurs.

Invites facultatives

Les invites facultatives suivantes sont compatibles avec l'enrôlement direct de Workspace ONE.

- Demander la propriété du terminal.
- Demander le numéro d'actif (uniquement prise en charge lorsque l'option Demander la propriété du terminal est activée.).
- Toutes les autres invites facultatives ne sont pas prises en charge.

Personnalisation

Les options de personnalisation suivantes sont compatibles avec l'enrôlement direct de Workspace ONE.

- Utiliser un modèle de message spécifique pour chaque plateforme.
- URL de redirection après l'enrôlement (iOS uniquement).
- Message de profil MDM (iOS uniquement).
- Utiliser les applications MDM personnalisées.
- Les options E-mail de support pour l'enrôlement et Numéro de téléphone de support pour l'enrôlement ne sont pas prises en charge.

Préenrôlement

Le préenrôlement de terminal via l'enrôlement direct de Workspace ONE n'est pas pris en charge. Si vous devez préenrôler un terminal pour un ou plusieurs utilisateurs, vous devez enrôler le terminal à l'aide de Workspace ONE Intelligent Hub au lieu d'utiliser l'enrôlement direct de Workspace ONE.

Profils du terminal

10

Les profils des terminaux sont votre principal moyen de gestion des terminaux dans Workspace ONE UEM powered by AirWatch. Ils représentent des paramètres facilitant l'application des procédures de l'entreprise, lorsqu'ils sont combinés à des politiques de conformité.

Créez des profils pour tous les types de plateforme et configurez une section de configuration qui correspond aux paramètres individuels que vous configurez pour chacun d'entre eux.

Le processus de création d'un profil consiste à d'abord définir les paramètres **généraux**, puis ceux de la **section de configuration**.

- Ces paramètres **généraux** déterminent la façon dont le profil est déployé et les utilisateurs qui le reçoivent.
- La **section de configuration** du profil correspond à la restriction elle-même et aux autres paramètres comme ils s'appliquent au terminal lorsque le profil est installé.

Ce chapitre contient les rubriques suivantes :

- Traitement du profil
- Ajouter des paramètres généraux de profil
- Affichage en liste des profils
- Version d'évaluation technique : profils et ressources de profil utilisés dans les workflows
- Modification du profil du terminal
- Profils de conformité
- Ressources du profil
- Zones de géo-barrière
- Horaires
- Afficher l'attribution des terminaux, profil de terminal

Traitement du profil

Les profils de terminaux fournissent une base normalisée pour la gestion des terminaux dans Workspace ONE UEM. Il est important de comprendre la méthode utilisée pour traiter les profils

de terminaux, notamment la logique de nouvelle tentative lorsque les installations de profil échouent.

Lorsqu'un profil de terminal est attribué à des terminaux, il est soumis au processus suivant.

1 Le profil est mis en file d'attente pour l'installation.

2 Le terminal se connecte aux services de terminaux, afin de recevoir le profil pour l'installation.
   - Si la connexion réussit, l'état d'installation du profil change et est défini sur « En attente ».
   - Si la connexion échoue, le profil est de nouveau mis en file d'attente pour l'installation (étape 1) lors du prochain archivage du terminal.

3 Le terminal installe le profil.
   - Si l'installation réussit, l'état d'installation du profil change et est défini sur « Traité ».
   - Si l'installation échoue, le profil est de nouveau mis en file d'attente pour l'installation (étape 1) lors du prochain archivage du terminal.

Réglage des performances

Le traitement et la publication de profils de terminaux, tels que des profils concernant des certificats, représentent une contrainte importante pour le serveur et doivent être régis pour alléger cette contrainte. Workspace ONE UEM Console utilise une logique de traitement par lots pour les types de profil de terminal consommant le plus de ressources processeur.

Cette logique de traitement par lots peut être ajustée en accédant à **Groupes et paramètres > Tous les paramètres > Installation > Réglage des performances**.

Paramètre	Description
Fréquence de validation pour la publication en masse	Les profils sont envoyés au nombre de terminaux entrés ici par transaction. La valeur minimale est 1000. La valeur maximale est 50 000. La valeur par défaut est 40 000.
Intervalle de la collecte du planificateur (en minutes)	Ce paramètre détermine la fréquence à laquelle le planificateur extrait un échantillon du terminal, mesurée en minutes. La valeur minimale est 1. La valeur maximale est 1 440 (24 heures). La valeur par défaut est 5.
Intervalle d'échantillonnage minimal (heures)	
Invitation de terminal iOS par seconde	Il s'agit du nombre de terminaux iOS par seconde qui sont invités à s'enregistrer dans les Services de terminaux par le biais d'un message sortant APN. La valeur minimale est 4. La valeur par défaut est 30. La valeur maximale recommandée est 120.
Fréquence de publication du profil du certificat	Il s'agit du nombre maximal de commandes d'installation de profil de certificat qui peuvent être publiées à tout instant pour l'ensemble de votre environnement. La valeur par défaut est 50.

Paramètre	Description
Nombre de commandes en file d'attente (max)	Il s'agit du nombre maximal de commandes que la file d'attente est autorisée à avoir. Les commandes sont publiées selon la fréquence de publication du profil de certificat jusqu'à ce qu'elles atteignent cette limite. Une fois que les terminaux consomment les commandes, plus de commandes sont mises en file d'attente. La valeur que vous entrez ici est multipliée par la « fréquence de publication du profil de certificat » pour obtenir ce nombre maximal. Ce nombre peut être augmenté pour améliorer le traitement par lot des certificats, mais vous devez envisager de surveiller étroitement les performances de l'autorité de certification et du serveur DS. La valeur par défaut est 10.
Restriction de la file d'attente de certificats	Si les commandes ajoutées par la fréquence de publication du profil de certificat ne sont pas consommées par les terminaux, le prochain lot est mis en file d'attente dans 15 minutes par défaut. Cet intervalle peut être abaissé pour améliorer le traitement par lot des certificats, mais vous devez envisager de surveiller étroitement les performances de l'autorité de certification et du serveur DS.
Seuil d'installation manuelle du profil de certificat	Il s'agit du nombre maximal de commandes d'installation de profil de certificat pouvant être mises en file d'attente à partir du tableau de bord par administrateur, par version de profil. La valeur par défaut est 100.
Maximum d'appels API d'Apple par seconde (pour inviter les utilisateurs VPP)	Spécifie le nombre maximal d'appels par seconde effectués sur les serveurs Apple VPP. La valeur minimale est 1. La valeur maximale est 1000. La valeur par défaut est 30.
Exécuter la conformité en temps réel	
Autoriser l'utilisation de minutes comme unité pour l'intervalle de temps pour la conformité	Activez pour créer des stratégies de conformité et définir des actions de hiérarchisation de conformité pour qu'elles s'effectuent à intervalle de temps basé sur une minute. Selon le nombre de terminaux enrôlés dans cet environnement, les performances de votre système peuvent être affectées. Tenez compte de ces facteurs avant d'activer cette option.
Taille du lot pour le déploiement d'applications internes	Cette valeur spécifie le nombre de terminaux qui sont inclus dans le lot pour le déploiement d'applications internes. La valeur minimale est 1. La valeur maximale est 10000. La valeur par défaut est 100.
Marquer la commande UEM d'application comme obsolète après	Cette limite de temps par plateforme définit la durée après laquelle la dernière commande UEM (reconnue par le terminal, mais pas encore exécutée) est considérée comme « obsolète ». Les commandes obsolètes sont redéclenchées une fois les applications publiées. Le catalogue d'applications n'affiche plus les applications dont l'état est « Traitement en cours » aux utilisateurs finaux, mais réactive plutôt les actions « Installer » ou « Mettre à jour ».
Intervalle des échantillons de la liste d'applications MDM (en minutes)	La valeur minimale est 1. La valeur par défaut est 480.
Heure de sondage d'échantillons de la liste d'applications Windows	La valeur minimale est 1. La valeur maximale est 1 440. La valeur par défaut est 5.

Paramètre	Description
Taille du lot pour la synchronisation des licences d'applications VPP	Ce paramètre spécifie le nombre d'applications incluses dans chaque lot lorsqu'elles se synchronisent avec le Cloud VPP. La valeur minimale est 1. La valeur maximale est 250. La valeur par défaut est 250.
Intervalle (en minutes) entre chaque nouvelle tentative après l'échec d'installation de l'application	Ce paramètre spécifie le délai d'attente avant de tenter une réinstallation d'une installation d'application ayant échoué. La valeur minimale est 15. La valeur maximale est 10000. La valeur par défaut est 60.
Nombre maximum de tentatives en cas d'échec d'installation des applications (Windows)	Spécifie le nombre maximal de nouvelles tentatives d'installation ayant échoué. La valeur minimale est 0. La valeur maximale est 8. La valeur par défaut est 5.
Taille du lot des terminaux pour les nouvelles tentatives en cas d'échec d'installation	Ce paramètre spécifie le nombre maximal de terminaux inclus dans une tentative de réinstallation d'une tentative d'installation d'application ayant échoué. La valeur minimale est 1. La valeur maximale est 15000. La valeur par défaut est 10000.
Fréquence (en heures) des mises à jour automatiques d'applications VPP basées sur les terminaux	Vous avez la possibilité de mettre à jour automatiquement les applications VPP basées sur un terminal. Ce paramètre contrôle la fréquence, exprimée en heures, à laquelle ces mises à jour se produisent. La valeur minimale est 1. La valeur maximale est 24. La valeur par défaut est 1.
Taille de la liste d'applications pour vérifier les mises à jour des versions des applications	Lorsque le système recherche une nouvelle version d'une application, ce paramètre spécifie la taille de la liste des applications qui sont vérifiées. La valeur minimale est 20. La valeur maximale est 100. La valeur par défaut est 20.
Installer les profils de certificat sans groupement lors de l'enrôlement	Détermine si les commandes de profil de certificat sont envoyées par lot. Lorsque cette option est activée, la logique de traitement par lot des commandes d'installation de profil de certificat pour les nouveaux enrôlements est ignorée. Lorsqu'elle est désactivée, la logique de traitement par lot des commandes d'installation de profil de certificat pour les nouveaux enrôlements est appliquée.
Intervalle de synchronisation (en heures) du nombre de licences VPP dans un groupe organisationnel	Il s'agit de la durée minimale, en heures, que le planificateur passe à sélectionner un groupe organisationnel pour exécuter le nombre de licences de synchronisation. La valeur minimale est 2. La valeur maximale est 24. La valeur par défaut est 6.
Nombre de groupes organisationnels par lot lors de la synchronisation du nombre de licences VPP	Il s'agit du nombre de groupes organisationnels que le planificateur peut sélectionner chaque fois qu'il exécute la tâche pour synchroniser le nombre de licences VPP. La valeur minimale est 1. La valeur maximale est 50. La valeur par défaut est 10.

Paramètre	Description
Suppression automatique d'un package de provisionnement Windows (PPKG) d'usine	Lorsque ce paramètre est activé, le module de provisionnement du produit qui est téléchargé sur le terminal est automatiquement supprimé, ce qui économise l'espace de stockage du terminal. Lorsqu'il est désactivé, le module PP est conservé sur le terminal.
Jours après lesquels les PPKG seront supprimés	Ce paramètre est disponible uniquement lorsque **Supprimer automatiquement le PPKG** est activé. Ce paramètre détermine le nombre de jours qui s'écoulent avant que le fichier PPKG soit supprimé du terminal. La valeur minimale est 0 (suppression immédiate). La valeur maximale est 90. La valeur par défaut est 5.
Taux de limitation de bande passante AWCM de provisionnement de produit	Représente le nombre de notifications de Messagerie Cloud d'AirWatch (AWCM) envoyées par seconde. Alignez ce taux de limitation avec la **taille des lots de lancement de commande de provisionnement de produit** par le tableau inclus **Dimensionnement de provisionnement de produit**. La valeur minimale est 1. La valeur maximale est 100. La valeur par défaut est 2.
Taille des lots de lancement de commande de provisionnement de produit	Les commandes de provisionnement de produit sont créées dans un état en attente. Ce paramètre représente le nombre de commandes lancées à partir de la file d'attente de commandes de terminal par intervalle de travail de libération de lot. La tâche du planificateur appelée « Travail de mise à jour de lot de provisionnement de produit » (dans **Groupes et paramètres > Tous les paramètres > Admin > Planificateur**) contrôle la fréquence de libération de la file d'attente de commandes. Ce paramètre contrôle le nombre de commandes lancées et alignées sur le **Taux de limitation de bande passante AWCM de provisionnement de produit** par intervalle. Les deux paramètres sont basés sur le nombre de serveurs de services de terminaux (DS) dans votre environnement, comme détaillé dans le tableau **Dimensionnement du provisionnement du produit**. La valeur minimale est 1. La valeur maximale est 10000. La valeur par défaut est 200.
Taille du lot d'installation du profil Apple	Cette valeur définit le nombre de commandes de profil qui sont ajoutées à la file d'attente de commande par lot. Ce paramètre est destiné à gérer le flux des commandes à traiter pour éviter l'expiration de la procédure. La valeur minimale est 300. La valeur maximale est 1000. La valeur par défaut est 300.

Dimensionnement de provisionnement de produit

Nombre de serveurs DS	Taux de limitation de bande passante AWCM	Taille des lots de lancement de commande
1	2	200
2	4	400
3	6	600
4	8	800
5	10	1000

Ajouter des paramètres généraux de profil

Les paramètres et options de profil suivants s'appliquent à la plupart des plateformes sous Workspace ONE UEM powered by AirWatch et peuvent être utilisés comme référence générale.

Cependant, certaines plateformes peuvent proposer des sélections différentes. Les étapes et paramètres s'appliquent à tous les profils.

Procédure

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

Vous pouvez choisir parmi les options suivantes pour ajouter un profil.

- **Ajouter un profil** – Ajoutez un nouveau profil de terminal.
- **Importer un profil** – Importez un profil signé sur votre terminal.
- **Importation par lot** – Importez de nouveaux profils de terminaux par lot en utilisant un fichier de valeurs séparées par des virgules (CSV). Saisissez un nom et une description uniques pour regrouper et organiser plusieurs profils à la fois.

2 Cliquez sur **Ajouter un profil**.

3 Sélectionnez la plateforme appropriée pour le profil que vous voulez déployer

En fonction de la plateforme, les paramètres de la section de configuration peuvent varier.

4 Sélectionnez l'onglet **Général** et complétez les paramètres suivants :

Paramètre	Description
Nom	Nom du profil qui s'affichera dans Workspace ONE UEM Console.
Version	Champ en lecture seule qui indique la version actuelle du profil, déterminée par l'option **Ajouter une version**.
Description	Brève description du profil qui en indique l'objectif.
Paramètres OEM (Android uniquement)	Activez ces paramètres pour configurer des profils propres aux terminaux Zebra et Samsung. S'ils sont activés, les profils sont signalés avec un symbole Knox pour indiquer les paramètres disponibles spécifiques à Knox. Deux nouveaux profils s'affichent : **Date/Heure** et **APN**. Ils sont spécifiques à Knox. Cette option apparaît uniquement lors de la configuration de profils Android.
Sélectionner OEM (Android uniquement)	Sélectionnez l'OEM **Samsung** ou **Zebra**. Cette option apparaît uniquement lors de la configuration de profils Android.
Déploiement	Détermine si le profil est automatiquement supprimé après désenrôlement (ne s'applique pas aux profils Android). ■ **Géré** – Le profil est supprimé. ■ **Manuel** – Le profil reste installé jusqu'à ce qu'il soit supprimé par l'utilisateur.
Portée du profil (Android ou Windows durci uniquement)	Détermine la façon dont le profil est utilisé. Sélectionnez l'une des options suivantes. ■ **Production** – Le profil sera utilisé dans le cadre du provisionnement de produits. ■ **Préenrôlement** – Le profil sera utilisé dans les configurations de préenrôlement. ■ **Les deux** – Le profil sera utilisé pour le préenrôlement et le provisionnement.

Paramètre	Description
Type d'attribution	Détermine la façon dont le profil est déployé sur les terminaux. ■ **Automatique** – Le profil est déployé sur tous les terminaux. ■ **Facultatif** – Le profil peut être installé de manière optionnelle par l'utilisateur depuis le portail en libre-service ou déployé vers des terminaux individuels à la discrétion de l'administrateur. Les utilisateurs finaux peuvent également installer des profils représentant des applications Web, à l'aide d'un raccourci Web ou d'une section de configuration de signets. Et si vous configurez la section de configuration à afficher dans le catalogue d'applications, vous pouvez l'installer à partir du catalogue d'applications. ■ **Interactif** – **(Ne s'applique pas à iOS ou Android)**. Ce profil est d'un type unique que les utilisateurs finaux installent à l'aide du portail en libre-service. Lorsqu'ils sont installés, ces types de profils spéciaux interagissent avec les systèmes externes pour générer des données à envoyer vers le terminal. Cette option n'est disponible que si vous l'activez dans **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Avancé > Options de profil**. ■ **Conformité** – Le profil est appliqué au terminal par le moteur de conformité lorsque l'utilisateur ne parvient pas à entreprendre les actions correctives permettant de rendre le terminal conforme. Pour plus d'informations, reportez-vous à la section Profils de conformité.
Autoriser la suppression	**(iOS 7 et versions antérieures uniquement)** Détermine si l'utilisateur final peut ou non supprimer le profil. ■ **Toujours** – L'utilisateur peut supprimer manuellement le profil à tout moment. ■ **Avec autorisation** – L'utilisateur peut supprimer le profil avec l'autorisation de l'administrateur. Si vous sélectionnez cette option, une zone de texte **Mot de passe** est ajoutée. ■ **Jamais** – L'utilisateur ne peut pas supprimer le profil du terminal.
Géré par	Groupe organisationnel disposant des droits d'administration pour le profil.
Groupes attribués	Groupes auxquels vous souhaitez ajouter le profil de terminal. Vous pouvez également créer un Smart Group et le configurer selon le système d'exploitation minimum, les modèles de terminaux, les catégories de propriété, les groupes organisationnels, etc. Même s'il s'agit d'un critère au sein d'un Smart Group, la plateforme configurée dans le profil de terminal ou la politique de conformité sera toujours prioritaire sur celle du Smart Group. Par exemple, si un profil de terminal est créé pour la plateforme iOS, il sera seulement attribué aux terminaux iOS même si le Smart Group comporte des terminaux Android.
Exclusions	Si **Oui** est sélectionné, un nouveau champ **Groupes exclus** s'affiche. Ce champ vous permet de sélectionner les groupes que vous souhaitez exclure de l'attribution du profil du terminal.
Afficher l'attribution des terminaux	Après avoir sélectionné le **groupe attribué**, vous pouvez prévisualiser une liste de tous les terminaux attribués, en tenant compte des attributions et exclusions de Smart Group.

Paramètre	Description
Critères d'attribution supplémentaires	Ces cases proposent des restrictions supplémentaires pour le profil. ■ **Installer uniquement sur les terminaux à l'intérieur des zones sélectionnées** – Saisissez une adresse dans le monde et un rayon en kilomètres ou en miles pour définir un « périmètre d'installation des profils ». Pour plus d'informations, reportez-vous à la section Zones de géo-barrière. ■ **Activer les horaires et installer le contenu uniquement pendant les périodes définies** – Définissez une période précise pendant laquelle les terminaux reçoivent le profil. En sélectionnant cette option, vous ajoutez un champ obligatoire **Horaires attribués**. Pour plus d'informations, consultez la section Horaires.
Date de suppression	Date à laquelle le profil est supprimé du terminal. La date doit être ultérieure et au format mm/jj/aaaa.

5 Définissez une **section de configuration** pour la plateforme de terminal. Vous pouvez rechercher une charge utile par nom en entrant des mots-clés dans la zone de texte **Rechercher une charge utile** au-dessus de la liste Charge utile.

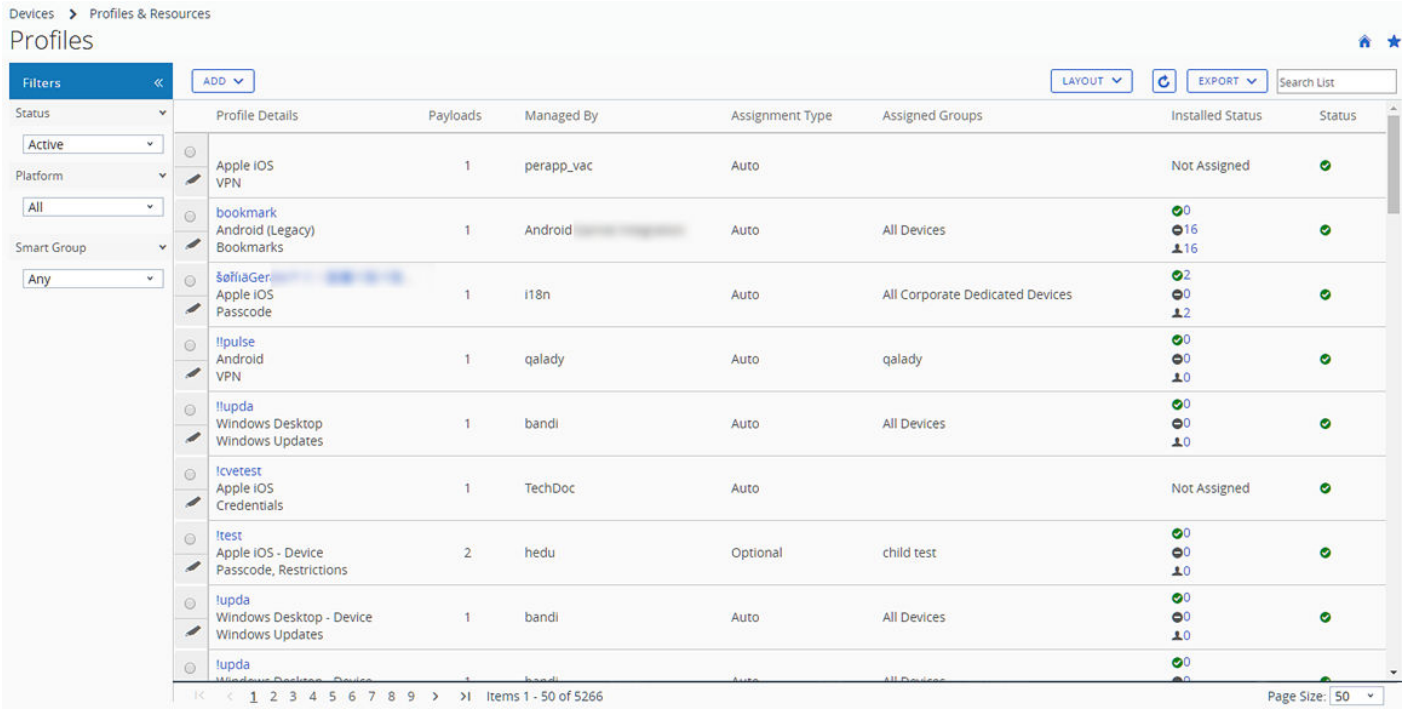
   Pour des instructions détaillées sur la configuration d'une **section de configuration** spécifique pour une plateforme donnée, consultez le **guide de la plateforme** concernée, disponible sur docs.vmware.com.

6 Cliquez sur **Enregistrer et publier**.

Affichage en liste des profils

Après avoir créé et attribué des profils dans Workspace ONE UEM, vous devez pouvoir gérer ces paramètres un par un et à distance depuis une source unique. La page **Ressources > Profils et lignes de base > Profils** propose un emplacement centralisé permettant d'organiser et de cibler les profils.

Vous pouvez créer des listes sur mesure de profils de terminaux selon les critères spécifiés en utilisant les **filtres**, la **mise en page** et le **tri de la colonne**. Vous pouvez aussi exporter ces listes sous un fichier CSV pour les afficher avec Excel, et voir le statut du profil du terminal.



Pop-up de pointage des profils de terminaux

Chaque profil de terminal de la colonne **Détails du profil** présente une icône d'info-bulle en haut à droite. Lorsque vous appuyez sur cette icône (terminal mobile tactile) ou passez le curseur de la souris dessus (PC ou Mac), un pop-up de pointage s'affiche.

Ce pop-up contient des informations de profil : **Nom de profil**, **Plateforme** et **Type** de la section de configuration incluse.

Une icône d'info-bulle semblable est également présente dans la colonne **Groupes attribués** de l'affichage en **liste des profils**, avec des pop-ups de pointage affichant les **Smart Groups attribués** et le **type de déploiement**.

Affichage en lecture seule des profils de terminaux

Les profils des terminaux créés dans et gérés par un groupe organisationnel sont en lecture seule lorsqu'un administrateur connecté avec un niveau de privilèges inférieur y accède. La fenêtre du profil indique cet état de lecture seule en ajoutant un commentaire spécial : « Ce profil est géré par un groupe organisationnel d'un niveau supérieur et ne peut pas être modifié. »

Cette limite de lecture seule s'applique également aux attributions de Smart Groups. Lorsqu'un profil est créé au niveau d'un groupe organisationnel parent et attribué à un Smart Group, un administrateur d'un sous-groupe organisationnel peut le consulter, mais ne peut pas le modifier.

Ce comportement assure le maintien d'une sécurité basée sur la hiérarchie et facilite la communication entre administrateurs.

Options de l'affichage en liste

Paramètre	Description
Filtres	Affichez seulement les profils souhaités en utilisant les filtres suivants. ■ **Statut** – Filtrez les terminaux pour afficher les appareils actifs, inactifs et tous les terminaux. ■ **Plateforme** – Filtrez les terminaux selon les 13 types de plateformes ou toutes les plateformes. ■ **Smart Group** – Filtrez les terminaux en sélectionnant un Smart Group depuis le menu déroulant.
Mise en page	Elle vous permet de personnaliser l'agencement des colonnes. ■ **Résumé** – Affichez les paramètres et les colonnes par défaut dans l'**affichage en liste**. ■ **Personnalisé** – Sélectionnez uniquement les colonnes de l'**affichage en liste** que vous voulez voir. Vous pouvez aussi appliquer les colonnes sélectionnées à tous les administrateurs au niveau du groupe organisationnel actuel ou en dessous de celui-ci.
Exporter	Enregistrez un fichier .xlsx ou .csv (valeurs séparées par des virgules) de l'intégralité de l'**Affichage en liste** qui peut ensuite être ouvert et analysé avec MS Excel. Si un filtre est appliqué à l'**affichage en liste**, la liste exportée sera également filtrée.
Tri de la colonne	Sélectionnez l'en-tête de colonne pour changer le tri de la liste.
Détails du profil	Dans les affichages **Résumé** et **Personnalisé**, la colonne **Détails du profil** affiche le nom, la plateforme et les types de charges utiles.
Charges utiles	Affiche le nombre de charges utiles spécifiées dans le profil de terminal.

Paramètre	Description
Statut de l'installation	Cette colonne affiche le statut de l'installation d'un profil grâce à trois indicateurs comportant chacun un lien hypertexte numérique. En cliquant sur ce lien, la page **Afficher les terminaux** s'affiche ; il s'agit d'une liste des terminaux concernés dans la catégorie sélectionnée. ■ **Installation en attente** () – Cet indicateur affiche le nombre de terminaux qui sont planifiés pour que le profil soit installé. ■ **Installé** () – Cet indicateur affiche le nombre de terminaux auxquels le profil a été attribué et sur lesquels il a été installé. ■ **Non installé** () – Cet indicateur affiche le nombre de terminaux auxquels le profil a été attribué mais sur lesquels il n'a pas été installé. ■ **Attribué** () – Cet indicateur affiche le nombre total de profils attribués, qu'ils soient installés ou non. ■ **Suppression en attente** () – Cet indicateur affiche le nombre total de profils planifiés pour la suppression. ■ **Supprimé(s)** () – Cet indicateur affiche le nombre total de profils supprimés. ■ **Obsolète(s)** () – Cet indicateur s'affiche lorsqu'une version mise à jour du profil installé est disponible. ■ **Informations en attente** () Cet indicateur s'affiche lorsque le profil est « en attente ». Voici des exemples typiques de cet état : les profils qui nécessitent des informations de serveurs tiers (tels que les profils VPN impliquant Websense et zScaler, ainsi que les profils de certificat nécessitant des données d'autorité de certification) restent dans un état en attente jusqu'à ce que le contact avec ces serveurs soit effectué et les informations requises soient obtenues. ■ **Non attribué** – Cet indicateur de texte s'affiche uniquement lorsque le profil a été défini et enregistré, mais pas encore attribué aux terminaux. ■ **Non applicable** – Cet indicateur texte s'affiche uniquement lorsque le profil est défini, enregistré et attribué, mais qu'il existe des détails dans sa configuration qui le rendent inapplicable aux terminaux auxquels il est attribué. ■ **Échec de l'installation** – Cet indicateur texte s'affiche uniquement lorsque le profil est défini, enregistré et attribué, mais qu'il existe une erreur qui l'empêche de s'installer correctement.

Case d'option et **icône Modifier**	L'**affichage en liste** comprend un bouton radio de sélection et une icône **Modifier** à gauche de chaque profil. Sélectionnez l'icône **Modifier** () pour modifier les paramètres de base de la configuration du profil. Si vous sélectionnez la case d'option, les boutons **Terminaux**, **XML** et **Plus d'actions** apparaissent au-dessus de la liste.
	■ **Terminaux** – Affichez les terminaux disponibles pour ce profil et si le profil est installé sur ceux-ci ; s'il ne l'est pas, vous pouvez également en afficher la raison. Surveillez les terminaux qui sont dans votre flotte et envoyez-leur manuellement des profils, si nécessaire.
	■ **</ > XML** – Affichez le code XML qu'Workspace ONE UEM génère après la création du profil. Affichez et enregistrez le code XML pour le réutiliser ou le modifier en dehors de la console.
	■ **Plus d'actions**
	  ■ **Copier** – Copiez un profil existant et modifiez la configuration de la copie pour démarrer rapidement avec les profils de terminaux.
	  ■ **Activer/Désactiver** – Rendez le profil de terminaux actif ou inactif.
	  ■ **Supprimer** – Maintenez votre tableau de profils en supprimant les profils inutiles.

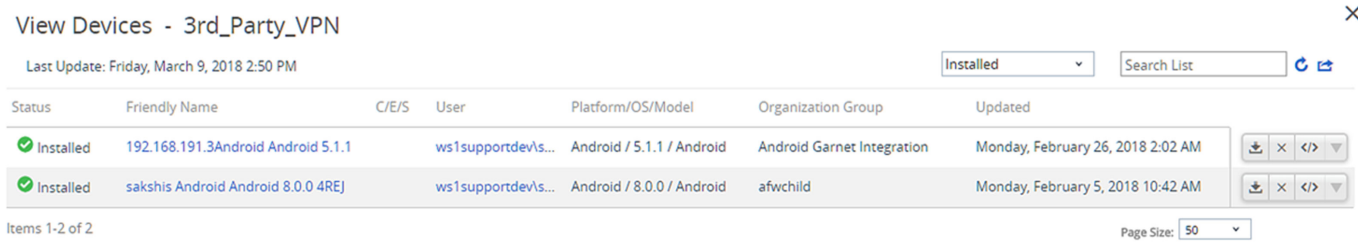
Confirmer l'installation du profil du terminal

Dans les situations peu fréquentes où les profils ne s'installent pas sur les terminaux ciblés, l'écran **Afficher les terminaux** vous permet d'en afficher les raisons.

État de l'installation du profil

1 Accédez à **Ressources > Profils et lignes de base > Profils** et observez la liste qui s'affiche.

2 Vérifiez la colonne **État de l'installation** et sélectionnez les liens numériques affichés à droite des icônes d'indicateur pour ouvrir l'écran **Afficher les terminaux**. Pour plus d'informations sur les icônes d'indicateur, reportez-vous aux définitions des **états d'installation** dans **Affichage en liste des profils**.



Résultat : l'écran **Afficher les terminaux - <profile name>** s'affiche.

3 (Facultatif) Générez un fichier CSV (Comma-Separated Value) de l'intégralité de la page **Afficher les terminaux** en sélectionnant l'icône **Exporter** ( ). Excel peut être utilisé pour lire et analyser le fichier CSV.

4 (Facultatif) Personnalisez les colonnes de la page **Afficher les terminaux** que vous souhaitez voir apparaître en sélectionnant l'icône **Colonnes disponibles** ( ).

Afficher la colonne Statut de la commande pour les terminaux iOS

Les terminaux iOS disposent d'une colonne **Statut de la commande** sur l'écran **Afficher les terminaux**. Elle inclut les statuts d'installation utiles pour le terminal iOS sélectionné. Les statuts suivants s'affichent dans la colonne Statut de la commande.

- **Erreur** – S'affiche en tant que lien qui affiche le code d'erreur applicable au terminal.
- **En attente** – S'affiche lorsque le terminal est inclus dans un processus global de certificat en cours.
- **Non applicable** – S'affiche lorsque l'attribution du profil n'a pas d'impact sur le terminal, mais qui fait néanmoins partie du Smart Group ou du déploiement. Par exemple, lorsque le type de profil n'est pas géré.
- **Plus tard** – S'affiche lorsque le terminal est verrouillé ou qu'il est occupé d'une autre manière.
- **En file d'attente** – S'affiche lorsque l'installation est en file d'attente et qu'elle est programmée.

- **Réussite** – S'affiche lorsque le profil a été installé avec succès.

Version d'évaluation technique : profils et ressources de profil utilisés dans les workflows

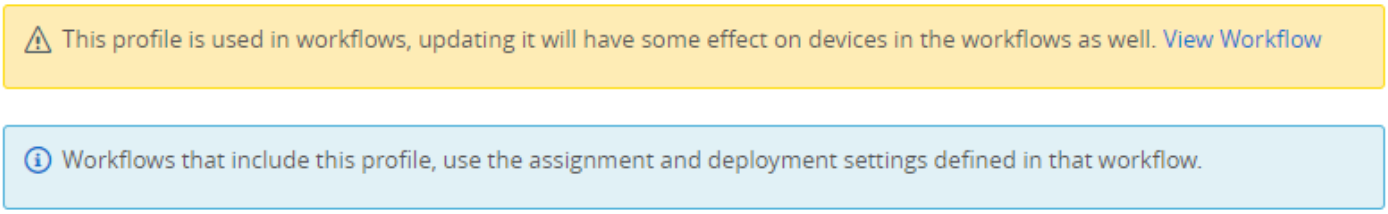
Vous pouvez voir le nombre de workflows Freestyle qui incluent un profil ou une ressource de profil en sélectionnant le profil dans l'affichage en liste et en sélectionnant le lien **Afficher le workflow**. Les modifications apportées aux profils de terminal et aux ressources de profil sont reflétées dans le workflow qui les utilise.

Note Workspace ONE UEM propose des workflows Freestyle Orchestrator en tant que fonctionnalités de la version d'évaluation technique pour nos clients SaaS. Pour plus d'informations, voir Qu'est-ce que Freestyle Orchestrator.

Les fonctionnalités de la version d'évaluation technique ne sont pas entièrement testées et certaines peuvent ne pas fonctionner comme prévu. Cependant, ces versions d'évaluation technique permettent à Workspace ONE UEM d'améliorer les fonctionnalités actuelles et de développer de futures améliorations. Le contenu de cette section concerne uniquement les clients qui participent à la version d'évaluation technique. Si vous participez à la version d'évaluation technique et que vous prévoyez d'utiliser une application ou une version spécifique d'une application dans les workflows, tenez compte des propriétés suivantes :

Notification pour les profils

Accédez à **Ressources > Profils et lignes de base > Profils**. Lorsque vous sélectionnez un profil de terminal qui est utilisé dans un workflow Freestyle, la notification suivante s'affiche.



Lorsque vous sélectionnez le lien **Afficher le workflow**, un écran **Workflow pour le profil** s'affiche, présentant tous les workflows Freestyle qui comportent le profil sélectionné, avec la description du workflow, les groupes attribués et la date de création du workflow.

Traitement en cours

Les profils qui font partie d'une attribution de Smart Group peuvent également être utilisés dans un workflow Freestyle. Pour les terminaux communs aux attributions de Smart Group et de workflow, le workflow est prioritaire,

sauf lorsque le **Type d'attribution** est défini sur « automatique », auquel cas l'attribution directe est prioritaire. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil** et, après que vous avez sélectionné la plateforme, l'option **Type d'attribution** est affichée dans l'écran **Charge utile générale**.

Apporter des modifications aux profils

Si vous apportez des modifications à un profil utilisé dans un workflow, ces modifications sont automatiquement répercutées dans le workflow.

Vous ne pouvez pas supprimer un profil qui est utilisé dans un Workflow. Vous devez d'abord supprimer le profil du workflow, ce que vous pouvez faire en modifiant le workflow. Pour plus d'informations, consultez le document Freestyle Orchestrator Guide.

Ressources du profil

De la même manière que les modifications apportées au profil de terminal affectent les workflows, si vous modifiez une ressource de profil Windows utilisée dans un workflow, les modifications sont répercutées dans le workflow.

Vous pouvez identifier le nom du workflow qui comporte la ressource de profil dans l'onglet **Attribution** de l'écran **Modifier la ressource**.

Pour plus d'informations sur les ressources de profil, reportez-vous à Ressources du profil.

Modification du profil du terminal

Avec Workspace ONE UEM powered by AirWatch, vous pouvez modifier un profil de terminal déjà installé sur les terminaux de votre flotte. Il existe deux types de modification que vous pouvez apporter au profil d'un terminal :

- **Général** – Les paramètres du profil permettent de gérer la distribution du profil : la manière dont il est attribué, le groupe organisationnel qui le gère, les Smart Groups auxquels il est attribué ou dont il est exclu.
- **Charge utile** – Les paramètres de profil de la charge utile affectent le terminal lui-même : la demande de code d'accès, les restrictions du terminal telles que l'utilisation de l'appareil photo ou la capture d'écran, les configurations Wi-Fi, le VPN, etc.

Le fonctionnement du terminal n'étant pas affecté, les changements apportés dans la section **Général** peuvent normalement être effectués sans republier le profil. La sauvegarde des changements entraînerait l'envoi du profil uniquement vers des terminaux qui n'ont pas encore été attribués au profil.

En revanche, les changements de la **section de configuration** doivent systématiquement être republiés vers tous les terminaux, les nouveaux comme ceux déjà existants, dans la mesure où le fonctionnement du terminal lui-même est affecté.

Modifier les paramètres des profils de terminaux

Les paramètres généraux de profil comprennent les modifications qui gèrent sa distribution uniquement. Cette distribution comprend la manière dont le profil est attribué, le groupe organisationnel qui le gère, le groupe d'attribution auquel il est attribué ou dont il est exclu.

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

2 Localisez le profil à modifier et sélectionnez l'icône **Modifier** associée ( ).

Les seuls profils modifiables sont ceux gérés par un groupe organisationnel (ou un sous-groupe organisationnel).

3 Procédez à tous les changements souhaités dans la catégorie **Général**.

4 Une fois les changements apportés à la catégorie **Général**, cliquez sur **Enregistrer et publier** afin d'appliquer le profil à tous les nouveaux terminaux que vous avez pu ajouter ou supprimer.

Les terminaux auxquels le profil a déjà été attribué reçoivent le profil republié. L'écran **Afficher l'attribution des terminaux** s'affiche, vous confirmant la liste des terminaux actuellement attribués.

Modifier les paramètres de profils de terminaux de la section de configuration

Les paramètres de profil de la section de configurations comportent des changements qui affectent le terminal lui-même : la demande de code d'accès, les restrictions du terminal telles que l'utilisation de l'appareil photo ou la capture d'écran, les configurations Wi-Fi, le VPN, etc.

Le bouton **Ajouter une version** vous permet de créer une nouvelle version du profil dont les paramètres de la **section de configuration** peuvent être modifiés.

1 Activez les modifications de la **section de configuration** qui affecte le fonctionnement du terminal en sélectionnant le bouton **Ajouter une version**.

Lorsque vous sélectionnez le bouton **Ajouter une version** et que vous enregistrez vos modifications, le profil est republié sur tous les terminaux auxquels il est attribué. Cette publication inclut les terminaux qui ont déjà le profil.

Pour des instructions détaillées sur la configuration d'une **section de configuration** spécifique, consultez le **guide de la plateforme** concernée disponible sur docs.vmware.com.

2 Une fois les modifications apportées à la **section de configuration**, cliquez sur **Enregistrer et publier** afin d'appliquer le profil à tous les terminaux attribués.

Résultat : l'écran **Afficher l'attribution des terminaux** s'affiche, vous confirmant la liste des terminaux actuellement attribués.

Profils de conformité

Pour comprendre les profils de conformité dans Workspace ONE UEM powered by AirWatch, vous devez comprendre les profils de terminaux et les stratégies de conformité. Les profils de terminaux servent de base pour la gestion et la sécurité des terminaux, tandis que les stratégies de conformité agissent comme une barrière de sécurité qui protège le contenu de l'entreprise.

Les profils de terminaux vous permettent de contrôler de nombreux paramètres de terminaux. Ces paramètres sont les suivants : complexité du code d'accès, géo-barrière, horaires, fonctionnalité du matériel du terminal, Wi-Fi, VPN, e-mail, certificats, etc.

Le moteur de conformité surveille les règles, effectue des opérations et applique des escalades (tous les éléments que vous définissez). Les profils de conformité cherchent toutefois à fournir au moteur de conformité l'ensemble des options et paramètres habituellement disponibles uniquement pour les profils de terminaux. Pour plus d'informations, reportez-vous à Chapitre 4 politiques de conformité.

Par exemple, vous pouvez créer un profil de terminal spécial, identique à votre profil de terminal normal, mais avec des paramètres plus restrictifs. Vous pouvez alors appliquer ce profil de terminal spécial dans l'onglet Actions lorsque vous définissez votre politique de conformité. Dans cette situation, si l'utilisateur ne parvient pas à rendre son terminal conforme, vous pouvez appliquer le profil de conformité le plus restrictif.

Ajouter un profil de conformité

Vous pouvez ajouter un profil de conformité, qui constitue un hybride entre une stratégie de conformité et le profil d'un terminal, associant le meilleur de ces deux fonctionnalités. L'ajout d'un profil de conformité est un processus en deux parties : (1) créer un profil de terminal et (2) l'attribuer en tant qu'action dans une stratégie de conformité.

Les profils de conformité sont créés et enregistrés comme les profils de terminaux Auto et Facultatif.

1 Accédez à **Ressources > Profils et lignes de base > Profils**, sélectionnez **Ajouter**, **Ajouter un profil**, puis sélectionnez une plateforme.

2 Sélectionnez un **nom** pour le profil de conformité que vous pouvez reconnaître ultérieurement.

3 Dans l'onglet de profil **Général**, sélectionnez Conformité dans le paramètre déroulant **Type d'attribution**.

4 Complétez les autres paramètres Général et Section de configuration.

5 Une fois que vous avez terminé, cliquez sur **Enregistrer et publier**.

6 Sélectionnez ce profil dans votre stratégie de conformité.

7 Accédez à **Terminaux > Stratégies de conformité > Affichage en liste**, sélectionnez **Ajouter**, puis sélectionnez une plateforme.

8 Définissez les **règles** et sélectionnez **Suivant**.

9 Dans l'onglet **Actions**, sélectionnez les options suivantes.

   a Définissez le menu déroulant sur Profil.

   b Définissez le deuxième menu déroulant sur Installer le profil de conformité.

   c Définissez le troisième menu déroulant sur le profil de terminal que vous avez nommé.

10 Sélectionnez **Suivant** et configurez les autres paramètres des onglets Attribution et Résumé.

11 Enregistrez la politique de conformité en sélectionnant **Terminer** ou **Terminer et activer**.

Pour des instructions détaillées sur la définition d'un profil de terminal, consultez Modification du profil du terminal.

Pour des instructions détaillées sur l'élaboration d'une stratégie de conformité, reportez-vous à la section Ajouter une politique de conformité.

Ressources du profil

Les ressources de profil facilitent le provisionnement des sections de configuration du Wi-Fi, du VPN et d'Exchange pour les déploiements Workspace ONE UEM qui prennent en charge plusieurs plateformes de terminaux, telles qu'iOS, Android et Windows.

Créez une ressource de profil pour l'une de ces sections de configuration et définissez les paramètres généraux reçus par chaque plateforme. Vous pouvez, si vous le voulez, configurer des paramètres propres à une plateforme en particulier afin qu'ils s'appliquent seulement à ces terminaux.

Les ressources de profil sont définies, gérées et déployées séparément des profils de terminaux. Déployez les ressources de profil avec les profils de terminaux pour offrir une gestion des terminaux à la fois large et détaillée pour toutes les plateformes supportées par votre déploiement.

Vous n'avez pas à utiliser de ressources de profil pour déployer les paramètres du Wi-Fi, du VPN ou d'Exchange. Si vous le souhaitez, vous pouvez toujours créer des profils de terminaux à part pour les sections de configuration de chaque plateforme. Envisagez le déploiement des ressources de profil lorsque vous pensez que les paramètres du Wi-Fi, du VPN ou d'Exchange sont identiques ou similaires à travers les plateformes. Puis, créez des profils de terminaux supplémentaires pour gérer plus de fonctionnalités pour chaque plateforme.

Affichage en liste des ressources de profil

Utilisez l'affichage en liste des ressources de profil de Workspace ONE UEM pour ajouter et gérer votre collection de ressources de profil comprenant l'affichage, la suppression et la modification des configurations pour les ressources individuelles.

Ajouter une ressource de profil

Vous pouvez ajouter une ressource de profil pour provisionner votre flotte de terminaux multi-plateforme avec les mêmes paramètres Exchange, Wi-Fi et VPN.

Accédez à **Terminaux > Ressources du profil** et sélectionnez **Ajouter une ressource**. Vous pouvez choisir parmi les options suivantes pour ajouter une ressource.

- **Exchange** – Configurez les paramètres des e-mails pour garder la connexion avec votre serveur de messagerie Exchange.
- **WiFi** – Configurez les paramètres de connectivité Wi-Fi afin de maintenir une connectivité réseau.
- **VPN** – Configurez les paramètres de réseau privé virtuel afin de maintenir une connexion sécurisée.

Chaque ressource de profil nécessite trois étapes de configuration distinctes. Créez une ressource de profil en précisant les **Détails de la ressource**, les **Plateformes** applicables et l'**Attribution** de la ressource aux terminaux.

- Les **Détails de la ressource** contiennent le nom de la ressource, sa description, les dépendances au serveur et d'autres paramètres essentiels qui déterminent le fonctionnement de la ressource de profil.
- Les **Plateformes** définissent sur quels terminaux la ressource de profil fonctionne.
- L'**Attribution** détermine la manière dont la ressource de profil est déployée, notamment les groupes organisationnels, les groupes d'utilisateurs et les Smart Groups.

Gérer les ressources

Une fois que vous avez accumulé un ensemble de ressources de profil, vous pouvez les gérer en accédant à **Terminaux > Ressources de profil**, puis les filtrer, les afficher, les modifier et les supprimer.

- **Filtrez** l'affichage en liste des ressources de profil pour voir celles qui sont actives, inactives ou les voir toutes.
- **Affichez** les différentes plateformes que votre ressource de profil comprend en sélectionnant le numéro d'hyperlien dans la colonne **Plateformes**.
  - Ouvrez la section **Paramètres avancés** pour la ressource de profil en sélectionnant le nom de la plateforme d'hyperlien.
  - Ouvrez la page **Afficher les terminaux** en sélectionnant les numéros d'hyperlien dans la colonne **Installés/attribués** de la page Plateformes. Cette page affiche la liste des terminaux attribués à la ressource de profil.
  - Affichez et exportez le code XML, et téléchargez un certificat en cliquant sur le lien hypertexte **Afficher** dans la colonne XML de la page des plateformes.
- **Modifiez** une ressource de profil en sélectionnant le lien de la ressource qui s'affiche dans la section **Détails de la ressource** de la page **Modifier la ressource**.
  - Modifiez les détails de la ressource de profil en cliquant sur l'icône Modifier () à gauche de la liste des ressources. Vous pouvez continuer à effectuer des modifications aux autres sections de la page **Modifier la ressource** en sélectionnant le bouton **Suivant**.

- Modifiez l'attribution de la ressource de profil en cliquant sur la case d'option à gauche de la liste de ressources de profil, puis en sélectionnant **Modifier l'attribution**.

- **Supprimez** une ressource de profil en cliquant sur la case d'option à gauche de la liste de ressources puis en sélectionnant **Supprimer**. La suppression d'une ressource la désactive jusqu'à ce qu'elle soit supprimée de tous les terminaux.

Ajouter une ressource Exchange

Vous pouvez ajouter une ressource destinée à assurer l'envoi et la réception de communications par e-mail sécurisées tout en étant gérée sous Workspace ONE UEM powered by AirWatch.

Pour un aperçu, reportez-vous à la section Ressources du profil.

Procédure

1 Accédez à **Terminaux > Profils et ressources > Ressources** et sélectionnez **Ajouter une ressource**, puis **Exchange** et renseignez les paramètres suivants.

Paramètre	Description
Détails de la ressource	
Nom de la ressource	Nom du profil qui s'affichera dans Workspace ONE UEM Console.
Description	Brève description du profil qui en indique l'objectif.
Informations de connexion	
Client de messagerie	Sélectionnez le client de messagerie que vous souhaitez utiliser avec la ressource.
Hôte Exchange	Saisissez l'hôte Exchange pour le compte de messagerie à inclure à la ressource.
Utiliser SSL	Activez le protocole SSL (Secure Socket Layer) pour ce client de messagerie.
Avancé	
Domaine*	Saisissez une valeur de recherche pour le domaine de messagerie.
Nom d'utilisateur*	Saisissez une valeur de recherche pour l'utilisateur de la messagerie.
Adresse e-mail*	Saisissez une valeur de recherche pour l'adresse e-mail.
Mot de passe	Saisissez un nom mot de passe pour le compte de messagerie. Cochez la case **Afficher les caractères** pour afficher le mot de passe.
Certificat d'identité	Importez et joignez une autorité de certification au compte de messagerie en sélectionnant le bouton **Ajouter un certificat**.
Synchronisation des e-mails depuis	Sélectionnez la longueur de la liste de l'historique de messagerie que vous voulez synchroniser. Choisissez entre **3 jours**, **1 semaine**, **2 semaines**, **1 mois** et **Illimité**.
Synchroniser le calendrier	Choisissez de synchroniser le calendrier du terminal avec le calendrier Exchange. Ce paramètre est activé par défaut sur les terminaux iOS et macOS.
Synchroniser les contacts	Choisissez de synchroniser les contacts du terminal avec les contacts Exchange. Ce paramètre est activé par défaut sur les terminaux iOS et macOS.

* Pour plus d'informations, reportez-vous à la section Chapitre 12 Valeurs de recherche.

2 Cliquez sur **Suivant** pour passer à la sélection des **plateformes**. Choisissez parmi les plateformes prises en charge, en optant pour les paramètres par défaut ou pour les **paramètres avancés**.

- **iOS.**

Paramètre	Description
Utilisez S/MIME.	Utilisez le protocole S/MIME, une clé publique de chiffrement et une norme de signature.
Certificat S/MIME	Cette option est disponible uniquement lorsque la fonction **Utiliser S/MIME** est activée. Ajoutez un certificat de signature aux e-mails en sélectionnant **Ajouter un certificat**.
Certificat S/MIME de chiffrement	Cette option est disponible uniquement lorsque la fonction **Utiliser S/MIME** est activée. Ajoutez un certificat pour le chiffrement et la signature numérique des e-mails en sélectionnant **Ajouter un certificat**.
Activez l'option « Par message ».	Cette option est disponible uniquement lorsque la fonction **Utiliser S/MIME** est activée. Donnez aux utilisateurs la possibilité de choisir les messages qu'ils souhaitent signer et chiffrer en utilisant le client de messagerie natif iOS (iOS 8 et versions ultérieures supervisées uniquement).
Paramètres et sécurité	
Empêchez le déplacement des messages.	Interdit le déplacement des e-mails depuis une boîte e-mail Exchange vers une autre boîte e-mail du terminal.
Empêchez l'utilisation dans des applications tierces.	Empêche les autres applications d'utiliser la boîte e-mail Exchange pour envoyer des messages.
Empêchez la synchronisation des adresses récentes.	Interdit les suggestions de contacts lors de l'envoi d'e-mails dans Exchange.
Empêchez le dépôt d'e-mails.	Interdit l'utilisation de la fonction Apple de dépôt de messages.

- **macOS.**

Paramètre	Description
Serveur Exchange interne	Nom du serveur sécurisé pour utiliser l'EAS Cette option et celle qui suivent s'affichent lorsque le **client de messagerie natif** est sélectionné.
Port	Saisissez le numéro de port attribué pour communiquer avec l'hôte Exchange externe.
Chemin d'accès interne au serveur	Emplacement du serveur sécurisé pour l'utilisation d'EAS
Utilisez SSL pour le serveur d'Exchange interne.	Communiquez avec l'hôte Exchange interne en activant le protocole SSL (Secure Socket Layer).
Hôte Exchange externe.	Nom du serveur externe pour l'utilisation d'EAS

Paramètre	Description
Port	Saisissez le numéro de port attribué pour communiquer avec l'hôte Exchange externe.
Chemin d'accès externe au serveur	Emplacement du serveur externe pour l'utilisation d'EAS
Utilisez SSL pour l'hôte Exchange externe.	Communiquez avec l'hôte Exchange externe en activant le protocole SSL (Secure Socket Layer).

- **Android.**

Paramètre	Description
Paramètres	
Nombre de jours passés pour lesquels synchroniser le calendrier	Sélectionnez un nombre de jours échus dans le calendrier sur le terminal.
Autoriser la synchronisation des tâches	Autorisez les tâches à se synchroniser avec le terminal.
Taille maximale de troncature d'e-mail (Ko)	Précisez la taille (en kilo-octets) au-delà de laquelle les e-mails sont tronqués lorsqu'ils se synchronisent avec le terminal.
Signature d'e-mail	Saisissez la signature d'e-mail à afficher dans le courrier sortant.
Ignorer les erreurs SSL	Autorisez les terminaux à ignorer les erreurs SSL pour les processus de l'Agent.
Restrictions	
Autoriser les pièces jointes	Autorisez les pièces jointes aux e-mails.
Taille maximale des pièces jointes	Définissez la taille maximum des pièces jointes en Mo.
Autoriser le transfert d'e-mails	Autorisez le transfert des e-mails.
Autoriser le format HTML	Précisez si l'e-mail synchronisé avec le terminal peut être au format HTML. Si ce paramètre est désactivé, tous les e-mails sont convertis en texte.
Désactiver les captures d'écran	Désactivez les captures d'écran sur le terminal.
Intervalle de synchronisation	Saisissez le nombre de minutes entre chaque synchronisation.
Jours de pointe pour la planification de la synchronisation	

Paramètre	Description
	■ Planifiez les jours de pointe pour la synchronisation, ainsi que l'**heure de début** et l'**heure de fin** de la synchronisation les jours sélectionnés. ■ Définissez la fréquence pour **Synchroniser le calendrier en heures de pointe** et**Synchroniser le calendrier en heures creuses**. ■ Le mode **Automatique** synchronise la messagerie à chaque mise à jour. ■ Le mode **Manuel** synchronise la messagerie uniquement à la demande. ■ L'indication d'une valeur de temps permet de synchroniser la messagerie selon une planification définie. ■ Activez les fonctions **Utiliser le SSL**, **Utiliser TLS** et **Compte par défaut**.
Paramètres S/MIME	
	Cliquez sur **Utiliser S/MIME**, puis sélectionnez un certificat S/MIME comme **Certificat utilisateur** dans la section de configuration **Identifiants**. ■ **Certificat S/MIME** – Sélectionnez le certificat à utiliser. ■ **Exiger le chiffrement des messages S/MIME** – Exige le chiffrement des messages S/MIME. ■ **Exiger la signature des messages S/MIME** – Exige la signature numérique de tous les messages S/MIME. Indiquez un **hôte de migration** si vous utilisez des certificats S/MIME pour le chiffrement.

- **Windows Desktop.**

Paramètres	Descriptions
Paramètres	
Prochain intervalle de synchronisation (min)	Sélectionnez la fréquence, en minutes, à laquelle le terminal se synchronise avec le serveur EAS.
Journalisation du diagnostic	Journalise les informations pour des raisons de dépannage.
Type de contenu	
Autoriser la synchronisation des e-mails	Autorise la synchronisation des e-mails.

3 Cliquez sur **Suivant** pour passer à la section **Attribution**.

4 Attribuez la ressource aux terminaux en complétant les paramètres suivants.

Paramètre	Description
Type d'attribution	Détermine la façon dont la ressource est déployée sur les terminaux. ■ **Automatique** – La ressource est déployée sur tous les terminaux automatiquement. ■ **Facultatif** – La ressource peut être installée de manière optionnelle par l'utilisateur depuis le portail en libre-service ou déployé vers des terminaux individuels à la discrétion de l'administrateur.
Géré par	Groupe organisationnel disposant des droits d'administration pour la ressource.

Paramètre	Description
Groupes attribués	Groupes auxquels vous souhaitez ajouter la ressource de terminal. Vous pouvez également créer un Smart Group et le configurer selon le système d'exploitation minimum, les modèles de terminaux, les catégories de propriété, les groupes organisationnels, etc.
Exclusions	Si vous sélectionnez **Oui**, la nouvelle zone de texte **Groupes exclus** s'affiche pour vous permettre de sélectionner les groupes que vous souhaitez exclure de l'attribution de la ressource du terminal.
Afficher l'attribution des terminaux	Après avoir effectué une sélection dans la zone de texte **Groupes attribués**, vous pouvez cliquer sur ce bouton pour prévisualiser la liste de tous les terminaux auxquels cette ressource est attribuée, en tenant compte des attributions et des exclusions de Smart Groups.

Ajouter une ressource Wi-Fi

Vous avez la possibilité d'ajouter une ressource dédiée aux terminaux dans le but de les connecter à un réseau sans fil, leur permettant ainsi d'envoyer et de recevoir des données en toute sécurité tout en étant gérée sous Workspace ONE UEM powered by AirWatch.

Pour un aperçu, reportez-vous à la section Ressources du profil.

Procédure

1 Accédez à **Terminaux > Profils et ressources > Ressources** et sélectionnez **Ajouter une ressource**, puis **Wi-Fi** et renseignez les paramètres suivants.

Paramètre	Description
Détails de la ressource	
Nom de la ressource	Nom du profil qui s'affichera dans Workspace ONE UEM Console.
Description	Brève description du profil qui en indique l'objectif.
Informations de connexion	
Identifiant SSID	Saisissez un identificateur associé au nom (SSID) du réseau Wi-Fi sécurisé.
Réseau masqué	Activez ce paramètre si le réseau n'est pas ouvert à la diffusion.
Rejoindre automatiquement	Paramètre indiquant au terminal de rejoindre le réseau automatiquement.
Chiffrement	Utilisez le menu déroulant pour indiquer si les données transmises utilisant la connexion Wi-Fi sont chiffrées. Apparaît en fonction du **Type de sécurité**.
Mot de passe	Saisissez un nom mot de passe pour le compte de messagerie. Cochez la case **Afficher les caractères** pour afficher le mot de passe.

2 Cliquez sur **Suivant** pour passer à la sélection des **plateformes**. Choisissez parmi les plateformes prises en charge, en optant pour les paramètres par défaut ou pour les **paramètres avancés**.

- **Configurer les paramètres avancés du proxy Wi-Fi.**

Paramètre	Description
Type de proxy	Choisissez entre **Aucun**, **Manuel** et **Automatique**.
URL du proxy	Disponible uniquement lorsque le **type de proxy** est **automatique**. Saisissez l'URL du proxy Wi-Fi utilisé par le terminal pour se connecter.
Autoriser une connexion directe si le PAC est inaccessible	Disponible uniquement lorsque le **type de proxy** est **automatique**. Activez ce paramètre si vous voulez autoriser votre terminal à se connecter en dehors des heures d'accessibilité du fichier de configuration automatique du proxy.
Serveur proxy	Disponible uniquement lorsque le **type de proxy** est **manuel**. Saisissez le nom du serveur proxy auquel vos terminaux se connectent.
Port du serveur proxy	Disponible uniquement lorsque le **type de proxy** est **manuel**. Indiquez le numéro de port du serveur proxy par lequel le terminal se connecte au serveur proxy.
Nom d'utilisateur proxy	Disponible uniquement lorsque le **type de proxy** est **manuel**. Saisissez un nom d'utilisateur reconnu par le serveur proxy.
Mot de passe proxy	Disponible uniquement lorsque le **type de proxy** est **manuel**. Saisissez le mot de passe correspondant au nom d'utilisateur saisi.

- **Configurer les paramètres avancés du Wi-Fi pour Android.**

Paramètre	Description
Fusion	
Inclure les paramètres de Fusion	Afficher les paramètres principaux pour la fonctionnalité Fusion.
Définir Fusion 802.11d / Activer 802.11d	Utilisez la norme de réseau sans fil 802.11d dans des domaines réglementaires supplémentaires.
Définir le code du pays / Code du pays	Définit le code du pays à utiliser dans les spécifications 802.11d.
Configurer la bande RF	Affiche toutes les options de spécification des fréquences radio, notamment le filtrage de fréquences 2,4 GHz et 5 GHz.
Définir 2,4 GHz / Activer 2,4 GHz	Utilise la fréquence sans fil 2,4 GHz.
Filtre de fréquence 2.4 Ghz	Réduit les interférences des canaux adjacents en appliquant le gabarit spectral ou le canal autour de la fréquence 2,4 GHz.
Définir 5 GHz / Activer 5 GHz	Utilise la fréquence sans fil 5 GHz.
Filtre de fréquence 5 Ghz	Réduisez les interférences des canaux adjacents en appliquant le gabarit spectral ou le canal autour de la fréquence 5 GHz.

Paramètre	Description
Proxy	
Activer le proxy en manuel	Affiche les paramètres du serveur proxy.
Serveur proxy	Saisissez le nom du domaine proxy.
Port du serveur proxy	Saisissez le numéro de port à utiliser par le serveur proxy.
Liste d'exclusions	Saisissez les nom d'hôte qui ne sont pas dirigés à travers le proxy. Utilisez un astérisque comme caractère générique pour le domaine. Par exemple, *.air-watch.com.

3 Cliquez sur **Suivant** pour passer à la section **Attribution**.

4 Attribuez la ressource aux terminaux en complétant les paramètres suivants.

Paramètre	Description
Type d'attribution	Détermine la façon dont la ressource est déployée sur les terminaux. ■ **Automatique** – La ressource est déployée sur tous les terminaux automatiquement. ■ **Facultatif** – La ressource peut être installée de manière optionnelle par l'utilisateur depuis le portail en libre-service ou déployé vers des terminaux individuels à la discrétion de l'administrateur.
Géré par	Groupe organisationnel disposant des droits d'administration pour la ressource.
Groupes attribués	Groupes auxquels vous souhaitez ajouter la ressource de terminal. Vous pouvez également créer un Smart Group et le configurer selon le système d'exploitation minimum, les modèles de terminaux, les catégories de propriété, les groupes organisationnels, etc.
Exclusions	Si vous sélectionnez **Oui**, la nouvelle zone de texte **Groupes exclus** s'affiche pour vous permettre de sélectionner les groupes que vous souhaitez exclure de l'attribution de la ressource du terminal.
Afficher l'attribution des terminaux	Après avoir effectué une sélection dans la zone de texte **Groupes attribués**, vous pouvez cliquer sur ce bouton pour prévisualiser la liste de tous les terminaux auxquels cette ressource est attribuée, en tenant compte des attributions et des exclusions de Smart Groups.

Ajouter une ressource VPN

Workspace ONE UEM powered by AirWatch vous permet d'ajouter une ressource dédiée pour fournir un réseau privé virtuel (VPN). Un VPN permet aux utilisateurs d'envoyer et de recevoir des données sur les réseaux publics comme s'ils étaient connectés directement à un réseau privé.

Pour un aperçu, reportez-vous à la section Ressources du profil.

Procédure

1 Accédez à **Terminaux > Profils et ressources > Ressources** et sélectionnez **Ajouter une ressource**, puis **VPN** et renseignez les paramètres suivants.

Paramètre	Description
Détails de la ressource	
Nom de la ressource	Nom du profil qui s'affichera dans Workspace ONE UEM Console.
Description	Brève description du profil qui en indique l'objectif.
Informations de connexion	
Type de connexion	Sélectionnez le type de connexion sécurisée dans la liste déroulante.
Serveur	Saisissez l'URL du serveur.

2 Cliquez sur **Suivant** pour passer à la sélection des **plateformes**. Choisissez parmi les plateformes prises en charge, en optant pour les paramètres par défaut ou pour les **paramètres avancés**.

- **iOS**
Paramètres	Description
Informations de connexion	
Compte	Saisissez le nom du compte VPN.
Déconnexion en cas d'inactivité (en minutes).	Autorisez le VPN à se déconnecter automatiquement après une certaine durée. La prise en charge de cette valeur dépend du fournisseur VPN.
Envoyer tout le trafic.	Sélectionnez ce paramètre pour forcer le trafic à travers un réseau spécifié.
Règles du VPN par application	Sélectionnez ce paramètre pour activer et configurer les règles du VPN par application.
Se connecter automatiquement.	Sélectionnez ce paramètre pour autoriser le VPN à se connecter automatiquement aux domaines Safari. Cette option s'affiche lorsque la case **Règles du VPN par application** est cochée.
Type de fournisseur	Sélectionnez le type de fournisseur VPN par application. Déterminez comment diriger le trafic, à travers une couche Application ou une couche IP, en sélectionnant AppProxy et PacketTunnel. Cette option s'affiche lorsque la case **Règles du VPN par application** est cochée.
Domaines pour Safari	Saisissez chaque domaine auquel vous voulez connecter automatiquement le VPN par application. Ces domaines sont des sites internes qui déclenche une connexion VPN automatique. Cette option s'affiche lorsque la case **Règles du VPN par application** est cochée.
Authentification	
Authentification utilisateur	Authentifiez les utilisateurs en important un **certificat** ou en exigeant un **mot de passe** pour l'accès VPN.
Nom de groupe	Saisissez le nom de groupe Workspace ONE UEM.

Paramètres	Description
Mot de passe	Disponible uniquement lorsque le paramètre **Authentification utilisateur** est défini sur Mot de passe. Saisissez le mot de passe du nom de groupe Workspace ONE UEM.
Certificat d'identité	Ce paramètre est disponible uniquement lorsque l'**authentification utilisateur** est définie sur Certificat. Sélectionnez **Ajouter un certificat** pour nommer ou importer un fichier de certificat ou choisir une autorité de certification existante à l'aide d'un modèle de certificat.
Activez le VPN à la demande.	Ce paramètre est disponible uniquement lorsque l'**authentification utilisateur** est définie sur Certificat. Activez le VPN à la demande afin d'utiliser des certificats pour établir automatiquement des connexions VPN.
Utiliser de nouvelles clés à la demande.	Ce paramètre est disponible uniquement lorsque l'**authentification utilisateur** est définie sur Certificat. Activez cette option pour lancer la connexion VPN lorsque les utilisateurs accèdent à l'un des domaines spécifiés.
Faire correspondre le domaine ou l'hôte.	Ce paramètre est disponible uniquement lorsque l'**authentification utilisateur** est définie sur Certificat. Saisissez un domaine ou un nom d'hôte, auquel un utilisateur accède, qui déclenche l'activation de la connexion VPN.
Action à la demande	Ce paramètre est disponible uniquement lorsque l'**authentification utilisateur** est définie sur Certificat. Sélectionnez l'action à la demande propre au domaine ayant lieu lorsque les utilisateurs activent une connexion VPN. Faites votre choix entre Toujours établir, Ne jamais établir et Établir si nécessaire.
Proxy	
Proxy	Faites votre choix entre **Aucun**, **Manuel** et **Automatique**.
URL de configuration automatique du serveur proxy	Disponible uniquement lorsque le **proxy** est **automatique**. Saisissez l'URL du proxy Wi-Fi utilisé par le terminal pour se connecter.
Serveur	Disponible uniquement lorsque le **proxy** est **manuel**. Saisissez le nom du serveur proxy auquel vos terminaux se connectent.
Port	Disponible uniquement lorsque le **proxy** est **manuel**. Indiquez le numéro de port du serveur proxy par lequel le terminal se connecte au serveur proxy.
Nom d'utilisateur	Disponible uniquement lorsque le **proxy** est **manuel**. Saisissez un nom d'utilisateur reconnu par le serveur proxy.
Mot de passe	Disponible uniquement lorsque le **proxy** est **manuel**. Saisissez le mot de passe correspondant au nom d'utilisateur saisi.
Configurations du fournisseur	
Clés du fournisseur	Créez des clés personnalisées à l'aide du dictionnaire de configuration du fournisseur.
Clé	Saisissez la clé spécifique fournie par le fournisseur.
Valeur	Saisissez la valeur VPN pour chaque clé.

- **Android**

Paramètre	Description
Authentification	
Certificat d'identité.	Cliquez sur **Ajouter un certificat** afin de saisir les identifiants de certificat utilisés pour authentifier la connexion.
Source des identifiants	Sélectionnez la source des identifiants. Faites votre choix entre Importer, Autorité de certification définie et Certificat utilisateur.
Nom des identifiants	Disponible lorsque la **source des identifiants** est définie sur Importer. Saisissez le nom des identifiants importés.
Certificat	Disponible lorsque la **source des identifiants** est définie sur Importer. Cliquez sur Importer pour sélectionner un fichier de certificat depuis votre terminal.
Autorité de certification	Disponible lorsque la **source des identifiants** est définie sur Autorité de certification définie. Sélectionnez l'autorité de certification dans le menu déroulant.
Modèle de certificat	Disponible lorsque la **source des identifiants** est définie sur Autorité de certification définie. Ce paramètre se remplit automatiquement en fonction de l'élément sélectionné dans Autorité de certification.
S/MIME	Disponible lorsque la **source des identifiants** est définie sur Certificat utilisateur. Choisissez entre le certificat de signature S/MIME propre à l'utilisateur ou le certificat de chiffrement S/MIME.
Activer le VPN à la demande	
Activez le VPN à la demande.	Activez le VPN à la demande afin d'utiliser des certificats pour établir automatiquement des connexions VPN. Activez le VPN à la demande en saisissant le nom de l'application et cliquant sur le signe Plus à gauche de la loupe. Vous pouvez ajouter plusieurs applications.

3 Cliquez sur **Suivant** pour passer à la section **Attribution**.

4 Attribuez la ressource aux terminaux en complétant les paramètres suivants.

Paramètre	Description
Type d'attribution	Détermine la façon dont la ressource est déployée sur les terminaux. - **Automatique** – La ressource est déployée sur tous les terminaux automatiquement. - **Facultatif** – La ressource peut être installée de manière optionnelle par l'utilisateur depuis le portail en libre-service ou déployé vers des terminaux individuels à la discrétion de l'administrateur.
Géré par	Groupe organisationnel disposant des droits d'administration pour la ressource.
Groupes attribués	Groupes auxquels vous souhaitez ajouter la ressource de terminal. Vous pouvez également créer un Smart Group et le configurer selon le système d'exploitation minimum, les modèles de terminaux, les catégories de propriété, les groupes organisationnels, etc.

Paramètre	Description
Exclusions	Si vous sélectionnez **Oui**, la nouvelle zone de texte **Groupes exclus** s'affiche pour vous permettre de sélectionner les groupes que vous souhaitez exclure de l'attribution de la ressource du terminal.
Afficher l'attribution des terminaux	Après avoir effectué une sélection dans la zone de texte **Groupes attribués**, vous pouvez cliquer sur ce bouton pour prévisualiser la liste de tous les terminaux auxquels cette ressource est attribuée, en tenant compte des attributions et des exclusions de Smart Groups.

Zones de géo-barrière

Workspace ONE UEM vous permet de définir votre profil avec une zone de géo-barrière, ce qui limite l'utilisation du terminal à des zones spécifiques. Vous pouvez vous représenter les zones de géo-barrières comme un périmètre virtuel pour une zone géographique réelle.

Par exemple, une zone de géo-barrières d'un rayon de 1 km peut s'appliquer à vos bureaux, tandis qu'une autre zone de géo-barrières beaucoup plus étendue peut s'appliquer à un pays tout entier. Une fois que vous avez défini une zone de géo-barrière, vous pouvez l'appliquer aux profils, aux applications SDK et aux applications Workspace ONE UEM.

- L'activation d'une zone de géo-barrière est une procédure en deux étapes.
  a Ajouter une zone de géo-barrière.
  b Appliquer une géo-barrière à un profil.
- Les géo-barrières sont disponibles pour les terminaux iOS et Android.
- Rappelez-vous que si les géo-barrières sont associées à une autre section de configuration activant les profils de sécurité en fonction de l'emplacement, nous vous conseillons tout de même de n'avoir qu'une section de configuration par profil.

Pour plus d'informations sur la manière dont Workspace ONE UEM suit les positions GPS, consultez l'article suivant, disponible sur la base de connaissance VMware AirWatch : https://support.workspaceone.com/articles/115001663108.

Ajouter une zone de géo-barrière

Vous devez définir une zone de géo-barrière avant de pouvoir l'appliquer à un terminal.

1 Affichez la page des paramètres Zone en accédant à **Ressources > Profils et lignes de base > Paramètres > Zones**.

Résultat : les paramètres système s'affichent.

2 Sélectionnez le bouton **Zone de géo-barrière**.

3 Saisissez une **adresse**, ainsi que le **rayon** de la géo-barrière (en kilomètres ou en miles).

Vous pouvez double-cliquer sur un emplacement de la carte pour définir le centre de la zone.

4 Sélectionnez **Cliquer pour rechercher** pour envoyer l'adresse entrée comme paramètre de recherche de Bing Maps. Si la recherche aboutit, la vue de carte se met à jour pour afficher l'emplacement entré avec l'adresse comme épicentre de la géo-barrière.

Note L'intégration à Bing maps implique que du « contenu non sécurisé » est chargé sur cette page. Si la recherche d'emplacement ne s'effectue pas comme prévu, vous devrez peut-être activer l'option « Afficher tout le contenu » dans votre navigateur.

5 Saisissez le **nom de la zone** (la manière dont elle s'affichera dans Workspace ONE UEM Console) et cliquez sur **Enregistrer**.

Que faire ensuite ? Vous devez maintenant appliquer une géo-barrière à un profil.

Application d'une géo-barrière à un profil

Une fois que vous avez ajouté une zone de géo-barrière, vous pouvez l'appliquer à un profil de sécurité et l'associer à d'autres sections de configuration pour créer des profils plus robustes.

Si un utilisateur désactive manuellement les services de localisation sur son terminal iOS, Workspace ONE UEM ne peut plus collecter les mises à jour de localisation. Workspace ONE UEM considère que le terminal se trouve à l'endroit où les services ont été désactivés.

1 Accédez à **Ressources > Profils et lignes de base > Profils** et localisez le profil auquel vous voulez appliquer une géo-barrière.

2 Sélectionnez l'icône de modification en forme de crayon ( ) du profil.

3 Sélectionnez **Installer uniquement sur les terminaux à l'intérieur des zones sélectionnées** dans l'onglet **Général**. Si cette case est désactivée, sélectionnez le bouton **Ajouter une version**. La création d'une nouvelle version implique la republication du profil.

Un champ **Zones de géo-barrières attribuées** s'affiche. Si aucune zone de géo-barrières n'a été définie, la console vous redirigera vers le menu de création de zones de géo-barrières.

4 Saisissez une ou plusieurs zones de géo-barrières dans ce profil.

5 Configurez une section de configuration, comme un code d'accès, des restrictions ou un réseau Wi-Fi, que vous souhaitez appliquer uniquement lorsque les terminaux se trouvent dans les zones de géo-barrières sélectionnées.

6 Cliquez sur **Enregistrer et publier**.

Par exemple, vous pouvez définir des zones de géo-barrières autour de chacun de vos bureaux. Ajoutez ensuite une section de configuration de restrictions pour désactiver l'accès au Game Center, aux jeux multi-joueurs ou au contenu YouTube, ainsi que d'autres paramètres. Une fois le profil activé, les employés du groupe organisationnel auxquels il est appliqué n'auront plus accès à ces fonctions tant qu'ils seront au bureau.

Prise en charge des géo-barrières sur les terminaux iOS

Les géo-barrières pour les applications ne fonctionnent que sur les terminaux iOS ayant activé les **services de localisation**. Pour que les services de localisation fonctionnent, le terminal doit être connecté à un réseau cellulaire ou à un point d'accès Wi-Fi. Dans le cas contraire, le terminal doit disposer de fonctions GPS intégrées.

Pour les terminaux connectés au Wi-Fi uniquement, la position GPS est signalée lorsque le terminal est allumé, déverrouillée, et Workspace ONE Intelligent Hub est ouvert et en cours d'utilisation. Les données GPS des téléphones mobiles sont envoyées lorsque le terminal change de tours de téléphonie mobile.

Le « mode avion » désactive les services de localisation (et par conséquent, des géo-barrières) sur le terminal.

Terminal	Wi-Fi	Réseau cellulaire	GPS intégré
iPhone	✓	✓	✓
iPad avec Wi-Fi et 3G/4G	✓	✓	✓
iPad avec Wi-Fi	✓		
iPod Touch	✓		

Toutes les conditions suivantes doivent être respectées pour que la position GPS se mette jour.

- Workspace ONE Intelligent Hub doit être en cours d'exécution sur le terminal.
- Les paramètres de confidentialité doivent permettre la collecte des données de localisation GPS (**Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Confidentialité**).
- Les paramètres de Workspace ONE Intelligent Hub pour Apple iOS doivent permettre la collecte des données de localisation (**Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Apple > Apple iOS > Paramètres du Hub**).

  Définissez les paramètres SDK de Workspace ONE Intelligent Hub sur les paramètres SDK par défaut au lieu de « Aucun ».

iBeacons

iBeacon est un protocole de détection de proximité basé sur le Bluetooth et développé par Apple. En tant que tel, il est exclusif à certains produits Apple.

iBeacon est propre à iOS et permet de gérer la connaissance des emplacements. Pour plus d'informations, consultez la section Aperçu d'Apple iBeacon.

Horaires

Alors qu'un profil sous Workspace ONE UEM powered by AirWatch détermine le niveau de restriction ou d'autorisation du terminal, les horaires soumettent l'application du profil à une

planification. Vous pouvez appliquer des horaires à un nouveau profil ou à un profil existant. Vous pouvez également supprimer des horaires inutilisés.

L'activation d'horaires est une procédure en deux étapes.

1 Définir des horaires

2 Appliquer des horaires à un nouveau profil ou à un profil existant

Définir des horaires

1 Accédez à **Ressources > Profils et lignes de base > Paramètres > Planification**.

2 Cliquez sur le bouton **Ajouter une planification**. L'écran **Ajouter une planification** s'affiche.

3 Sélectionnez le bouton **Ajouter une planification** situé dans la colonne **Jour de la semaine**, puis complétez les paramètres suivants.

Paramètre	Description
Nom de la planification.	Saisissez le nom de la planification qui apparaît dans l'affichage en liste des terminaux.
Fuseau horaire	Sélectionnez le fuseau horaire du groupe organisationnel sous lequel le terminal est géré.
Jour de la semaine	Appliquez une installation de profil planifiée en sélectionnant un jour de la semaine.
Toute la journée	Installez le profil à minuit le **jour de la semaine** sélectionné. En cochant cette case, vous supprimez les colonnes **Heure de début** et **Heure de fin**.
Heure de début.	Sélectionnez l'heure souhaitée d'installation du profil.
Heure de fin.	Sélectionnez l'heure souhaitée de désinstallation du profil.
Actions	Supprimez l'horaire du jour en cliquant sur **X**.

4 Cliquez sur **Enregistrer**.

Appliquer des horaires à un profil

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

2 Cochez **Activer les horaires et installer le contenu uniquement pendant les périodes définies** dans l'onglet **Général**.

3 Dans le champ **Horaires attribués**, saisissez un ou plusieurs horaires pour ce profil.

4 Configurez une section de configuration, comme un code d'accès, des restrictions ou un réseau Wi-Fi, que vous souhaitez appliquer aux terminaux uniquement pendant les périodes indiquées.

5 Cliquez sur **Enregistrer et publier**.

Appliquer des horaires à un profil existant

1 Accédez à **Ressources > Profils et lignes de base > Profils** et recherchez le profil à modifier dans la liste. Modifiez le profil en cliquant sur l'icône en forme de crayon ( ) ou cliquez sur le nom du profil.

2 Dans l'onglet **Général** de la page des profils, activez le paramètre **Activer les horaires et installer le contenu uniquement pendant les périodes définies**.

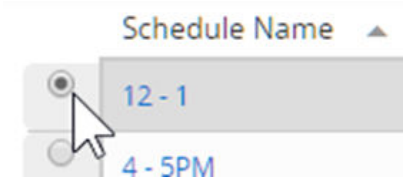
3 Dans le paramètre **Horaire attribué** qui s'affiche, sélectionnez dans le menu déroulant celui précédemment enregistré.

4 Cliquez sur **Enregistrer et publier**.

Supprimer des horaires

1 Accédez à **Ressources > Profils et lignes de base > Paramètres > Planification**.

2 Sélectionnez le bouton radio situé à côté de l'horaire à supprimer.



3 Sélectionnez le bouton **Supprimer**.

Afficher l'attribution des terminaux, profil de terminal

La sélection du bouton **Enregistrer et publier** lors de la configuration d'un profil de terminal affiche l'écran **Afficher l'attribution des terminaux**. Cet écran affiche un aperçu des terminaux gérés par Workspace ONE UEM powered by AirWatch qui sont affectés (ou non affectés) par l'attribution de profil de terminal.

Selon le type de changements apportés au profil du terminal, la colonne **Statut de l'attribution** affiche différents éléments.

- **Ajouté** – Le profil est ajouté et publié sur le terminal.
- **Supprimé** – Le profil est supprimé du terminal.
- **Inchangé** – Le profil n'est pas republié sur le terminal.
- **Mis à jour** – Le profil est republié sur un terminal auquel il est déjà attribué.

Cliquez sur **Publier** pour finaliser les modifications et, le cas échéant, republier tous les profils nécessaires.

Balises de terminal

11

Les balises de terminal dans Workspace ONE UEM powered by AirWatch vous permettent d'identifier un terminal sans profil, Smart Group ni stratégie de conformité, et ce, sans devoir créer de note.

Vous pouvez filtrer l'affichage en liste des terminaux par balises, attribuer des balises à un ou plusieurs terminaux, annuler l'attribution de balises et supprimer des balises non attribuées.

Par exemple, si des terminaux présentent une batterie obsolète ou un écran cassé, les balises permettent de les identifier dans la console. Une autre fonction consiste à identifier les variantes de matériel d'une manière plus visible plutôt que de se baser sur le numéro de modèle ou la description pour distinguer les terminaux.

Par exemple, deux terminaux Windows Desktop peuvent avoir le même numéro de modèle, mais un processeur légèrement différent ou encore une mémoire ou une carte vidéo personnalisée. Le balisage du matériel permet une identification facile de ces terminaux dans la console.

Étiquettes et Smart Groups

La fonctionnalité de balisage est intégrée aux Smart Groups. Cette intégration signifie que les balises peuvent être utilisées pour définir un Smart Group.

Par exemple, si vous avez balisé tous les terminaux de votre flotte qui présentent des dégâts visibles, vous pouvez les regrouper dans un Smart Group et les exclure de l'ensemble des terminaux. Vous pouvez alors exclure ce Smart Group du groupe des terminaux que vous attribuez temporairement aux visiteurs du site.

Une autre possibilité consiste à étiqueter les terminaux moins performants. Vous pouvez créer un Smart Group avec ces terminaux balisés et les exclure des attributions pour les missions stratégiques.

Balises de terminal et autorisations de rôle

Toutes les activités associées à la fonctionnalité de balise de terminal nécessitent des autorisations sur le rôle que vous attribuez à vos administrateurs. Si vous souhaitez que la responsabilité de création de balises incombe à vos administrateurs, vous devez ajouter cette autorisation (également appelée Ressources dans le console) au rôle que vous attribuez à l'administrateur concerné. Il en va de même pour l'affichage, la modification, la suppression, l'attribution de balises, et même la possibilité de les rechercher.

Filtrer les terminaux par étiquette

1 Accédez à **Terminaux > Affichage en liste** et cliquez sur **Filtres**. La colonne **Filtres** s'affiche à gauche de la liste de terminaux.

2 Sélectionnez **Avancé** dans la liste des catégories de filtre et choisissez **Étiquettes**.

3 Cliquez n'importe où dans la zone de texte de recherche et sélectionnez un terminal dans la liste qui s'affiche.

Résultat : les terminaux dont les balises ne sont pas sélectionnées sont exclus de la liste de résultats. L'**affichage en liste des terminaux** se met à jour automatiquement dès que la première étiquette est sélectionnée.

Créer une nouvelle balise à partir des Paramètres système

Avant de commencer : vous devez disposer des autorisations appropriées pour créer une balise. Vous pouvez vérifier ces autorisations en affichant toutes les ressources (ou autorisations) attribuées à un rôle d'administrateur, modifier le rôle avec l'autorisation « Créer une balise » et, si ce n'est pas déjà fait, attribuer ensuite le rôle modifié à votre compte d'administrateur. Pour plus d'informations, reportez-vous à la section **Afficher les ressources d'un rôle d'administrateur**.

1 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Avancé > Balises**.

2 Cliquez sur le bouton **Créer une balise**. L'écran **Créer une balise** s'affiche.

3 Saisissez le **nom** de l'étiquette ; La sélection du nom de la balise est ce qui la rend utile ou non. Sélectionnez un nom pouvant être utilisé pour identifier un terminal d'un coup d'œil.

4 Sélectionnez le **Type** de balises que vous souhaitez : **Terminal**, **Général** ou **Vidéo**.

5 Cliquez sur **Enregistrer**.

La balise de terminal est maintenant disponible pour être attribuée à un terminal. Accédez à **Terminaux > Affichage en liste** et sélectionnez un ou plusieurs terminaux auxquels attribuer cette balise.

Attribuer des balises à un seul terminal

Vous pouvez attribuer des balises à un terminal pour l'identifier sans utiliser de notes, de profils, de politiques, ni lui donner de nom convivial. Vous cherchez à octroyer des autorisations dans le cadre d'un rôle d'administrateur qui inclut (ou exclut) la possibilité d'attribuer une balise à un terminal ? Reportez-vous à la rubrique **Afficher les ressources d'un rôle d'administrateur**.

1 Accédez à **Terminaux > Affichage en liste** et choisissez le terminal que vous souhaitez étiqueter. Sélectionnez le terminal que vous souhaitez baliser en choisissant entre ces deux méthodes de sélection.

   a Sélectionnez le nom convivial du terminal dans la liste pour afficher la **Affichage des détails**.

   b Cochez la case au-dessus de l'icône de crayon, en regard du terminal.

2 Cliquez sur le bouton **Plus d'actions**, puis sur **Attribuer une balise**. L'écran **Attribution des étiquettes** apparaît avec une liste d'étiquettes pouvant être appliquées au terminal choisi.

3 Choisissez chacune des étiquettes que vous souhaitez attribuer au terminal. Il est possible d'en sélectionner plusieurs. Si vous avez sélectionné **Attribuer une balise** à partir de l'**Affichage des détails** du terminal, vous disposez également d'un lien **Gérer les balises** qui, lorsque cette option est sélectionnée, ouvre la page Paramètres système des balises, vous permettant de créer une nouvelle balise.

Attribuer des balises à plusieurs terminaux.

Vous devez disposer des autorisations adéquates pour attribuer une balise à plusieurs terminaux. Vous pouvez vérifier ces autorisations en affichant toutes les ressources (ou autorisations) attribuées à un rôle d'administrateur, modifier le rôle avec l'autorisation « Gestion en masse d'attributions de balises aux terminaux » et, si ce n'est pas déjà fait, attribuer ensuite le rôle modifié à votre compte d'administrateur.

Vous pouvez configurer le nombre maximal de terminaux auxquels vous êtes autorisé à attribuer ou supprimer des balises en accédant à **Groupes et Paramètres > Tous les paramètres > Terminaux et Utilisateurs > Avancé > Gestion en masse**, puis défilez vers le bas jusqu'à l'option **Attribuer/Annuler l'attribution de la balise**.

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

2 Cochez la case en regard de chaque terminal que vous souhaitez étiqueter.

3 Cliquez sur **Plus d'actions**, puis sur **Gérer les balises**.

   La page **Gérer les balises** s'affiche avec plusieurs éléments d'information. Elle confirme le nombre de terminaux sélectionnés dans l'affichage en liste, et indique les balises actuellement attribuées ou disponibles à l'attribution. Vous pouvez également utiliser les champs de recherche dans le coin supérieur droit de la page Gérer les balises pour saisir les paramètres de recherche des étiquettes de balises.

4 Sélectionnez les étiquettes que vous souhaitez attribuer à tous les terminaux choisis. Il est possible d'en sélectionner plusieurs. Vous pouvez également attribuer des balises et annuler l'attribution d'autres balises à la même étape.

5 Cliquez sur **Enregistrer**.

Modifier une balise de terminal existante

Vous devez disposer des autorisations appropriées pour modifier une balise. Vous pouvez vérifier ces autorisations en affichant toutes les ressources (ou autorisations) attribuées à un rôle d'administrateur, modifier le rôle avec l'autorisation « Modifier une balise » et, si ce n'est pas déjà fait, attribuer ensuite le rôle modifié à votre compte d'administrateur.

1 Accédez à **Groupes et paramètres > Terminaux et utilisateurs > Avancé > Balises**.

2 Identifiez la balise que vous souhaitez modifier dans la liste.

3 Sélectionnez l'icône de crayon (✎) en regard de la balise que vous souhaitez modifier. L'écran Modifier une balise s'affiche.

4 Modifiez le **Nom** de la balise.

5 Cliquez sur **Enregistrer**.

Résultat : la balise a été modifiée, un nouveau nom lui a été attribué. Les terminaux auxquels la balise étaient attribués ont été mis à jour avec la balise modifiée.

Annuler l'attribution de balises à plusieurs terminaux

Vous devez disposer des autorisations adéquates pour annuler l'attribution d'une balise à plusieurs terminaux. Vous pouvez vérifier ces autorisations en affichant toutes les ressources (ou autorisations) attribuées à un rôle d'administrateur, modifier le rôle avec l'autorisation « Gestion en masse d'annulations d'attributions de balises » et, si ce n'est pas déjà fait, attribuer ensuite le rôle modifié à votre compte d'administrateur. Pour plus d'informations, reportez-vous à la section **Afficher les ressources d'un rôle d'administrateur**.

Vous pouvez configurer le nombre maximal de terminaux auxquels vous êtes autorisé à attribuer ou supprimer des balises en accédant à **Groupes et Paramètres > Tous les paramètres > Terminaux et Utilisateurs > Avancé > Gestion en masse**, puis défilez vers le bas jusqu'à l'option **Attribuer/Annuler l'attribution de la balise**.

Pour annuler l'attribution de balises à plusieurs terminaux, procédez aux étapes suivantes.

1 Accédez à **Terminaux > Affichage en liste**, puis recherchez la balise dont vous souhaitez annuler l'attribution. Vous pouvez également filtrer les terminaux en fonction d'une ou de plusieurs balises.

2 Cochez la case située à gauche de chaque terminal dans l'Affichage en liste des terminaux contenant la balise dont vous souhaitez annuler l'attribution.

3 Sélectionnez le bouton **Plus d'actions** au-dessus de la liste.

4 Sélectionnez **Gérer les balises**.

La page **Gérer les balises** s'affiche avec plusieurs éléments d'information. Elle confirme le nombre de terminaux sélectionnés dans l'affichage en liste, et indique les balises actuellement attribuées ou disponibles à l'attribution. Vous pouvez également utiliser les champs de recherche dans le coin supérieur droit de la page Gérer les balises pour saisir les paramètres de recherche des étiquettes de balises.

5 Sélectionnez le petit x en regard de chaque balise attribuée que vous souhaitez supprimer. Il est possible d'annuler l'attribution de plusieurs balises. Vous pouvez également attribuer des balises et annuler l'attribution d'autres balises à la même étape.

6 Cliquez sur **Enregistrer**.

Résultat : l'attribution de la balise a été annulée de tous les terminaux sélectionnés. Si cette balise est attribuée à un autre terminal, la balise ne peut pas être supprimée.

Supprimer une balise de terminal non attribuée (inutilisée)

Tant qu'une balise n'est pas attribuée et que vous n'avez pas prévu de l'utiliser de nouveau, vous pouvez la supprimer.

Vous devez disposer des autorisations appropriées pour supprimer une balise. Vous pouvez vérifier ces autorisations en affichant toutes les ressources (ou autorisations) attribuées à un rôle d'administrateur, modifier le rôle avec l'autorisation « Supprimer une balise » et, si ce n'est pas déjà fait, attribuer ensuite le rôle modifié à votre compte d'administrateur. Pour plus d'informations, reportez-vous à la section **Afficher les ressources d'un rôle d'administrateur**.

Les balises que vous souhaitez supprimer ne doivent être attribuées à aucun terminal.

Pour annuler l'attribution de balises de certains terminaux, reportez-vous à la section précédente ci-dessus.

1 Une fois l'annulation de l'ensemble des attributions de la balise effectuée, accédez à **Groupes et paramètres > Terminaux et utilisateurs > Avancé > Balises**.

2 Identifiez la balise que vous souhaitez supprimer de la liste.

3 Sélectionnez le bouton radio en regard de la balise à supprimer. Le bouton **Supprimer** s'affiche au-dessus de la liste.

4 Cliquez sur **Supprimer**. Une confirmation demandant « Supprimer la balise définitivement ? s'affiche »

5 Sélectionnez **OK** sur la confirmation. Si la balise est attribuée à un terminal, vous n'êtes pas autorisé à la supprimer. Reportez-vous aux instructions ci-dessus pour annuler l'attribution de balises à des terminaux.

Si la balise n'est attribuée à aucun terminal lorsque vous la supprimez, elle est alors supprimée.

Valeurs de recherche

12

Une valeur de recherche est une variable qui représente un élément de données particulier d'un compte de terminal, d'utilisateur ou d'administrateur dans Workspace ONE UEM et dans Workspace ONE Express. Les valeurs de recherche peuvent être précieuses pour compléter un processus ou un formulaire.

Dans plusieurs zones de texte différentes de Workspace ONE UEM Console et de Workspace ONE Express, vous pouvez ajouter des valeurs de recherche à la place de valeurs statiques ou saisies manuellement. Dans la plupart des cas, les valeurs de recherche remplacent une information que vous ne connaissez pas ou à laquelle vous n'avez pas accès.

Par exemple, l'écran **Ajouter un terminal** est utilisé pour ajouter un terminal à votre flotte. **Nom convivial attendu** est l'une des zones de texte de cet écran qui peuvent être renseignées avec des valeurs de recherche.

Le nom convivial désigne le terminal sur de nombreux écrans différents d'UEM Console, y compris **Affichage en liste des terminaux** et **Affichage détaillé**. Vous pouvez saisir un nom convivial statique manuellement lorsque vous ajoutez un terminal, mais vous pouvez aussi utiliser des valeurs de recherche pour standardiser le nom convivial et en faire un identificateur important.

Un format de nom convivial courant peut être construit avec les valeurs de recherche suivantes.

```
{EnrollmentUser} {DeviceModel} {DeviceOperatingSystem} {DeviceSerialNumberLastFour}
```

Si vous entrez cette chaîne dans la zone de texte **Nom convivial attendu**, un nom convivial semblable à celui de la fenêtre **Affichage en liste des terminaux** apparaît.

```
jsmith iPad iOS GHKD
```

Ce nom convivial vous fournit instantanément au moins trois informations utiles. Avec les quatre derniers chiffres du numéro de série de terminal ajoutés à la fin, il est pratiquement certain que ce nom est unique.

Capacité supplémentaire de données

Lorsqu'elles sont utilisées, les valeurs de recherche n'ajoutent pas une charge supplémentaire à la mémoire du terminal. Les valeurs de recherche sont une construction de Console, et non des données transférées vers le terminal.

Chaînes statiques et valeurs de recherche

Les valeurs de recherche ne peuvent pas être appliquées une fois qu'une chaîne statique a été entrée dans une zone de texte.

Par exemple, supposons que vous avez 100 terminaux à enrôler. Vous ajoutez les 50 premiers à l'aide d'une chaîne statique entrée manuellement dans **Nom convivial attendu**. Pour les 50 suivants, vous choisissez d'utiliser une valeur de recherche pour le **nom convivial attendu**. Ces 100 terminaux, parmi lesquels une moitié dispose de noms conviviaux statiques et l'autre de valeurs de recherche, peuvent tout à fait coexister. Cela ne pose aucun problème d'associer des chaînes statiques avec des valeurs de recherche.

Cependant, vous ne pouvez pas revenir aux 50 premiers terminaux et remplacer le nom convivial de la chaîne statique par une valeur de recherche.

Valeurs de recherche personnalisées

Vous pouvez utiliser la fonctionnalité Attributs personnalisés pour créer vos propres valeurs de recherche. Vous pouvez ensuite utiliser ces valeurs de recherche personnalisées de la même manière que les valeurs de recherche ordinaires.

Confidentialité pour les déploiements de terminaux personnels

13

L'une des plus grandes préoccupations des utilisateurs finaux qui utilisent des terminaux personnels est la confidentialité du contenu personnel sur leurs terminaux gérés par Workspace ONE UEM. Votre organisation doit garantir aux employés que leurs données personnelles ne sont pas soumises à la supervision de l'entreprise.

Avec Workspace ONE UEM, vous pouvez garantir la confidentialité des données personnelles en créant des stratégies de confidentialité personnalisées qui ne collectent pas de données personnelles en fonction du type de propriété du terminal. En outre, vous pouvez définir des paramètres de confidentialité granulaire pour désactiver la collecte des informations de nature à identifier personnellement et interdire certaines actions distantes sur des terminaux détenus par des employés afin de garantir la confidentialité de ces derniers.

Vous devez informer vos employés de la manière dont leurs données sont collectées et stockées lorsqu'ils s'enrôlent dans Workspace ONE UEM.

Pour plus d'informations sur la manière dont VMware traite les données collectées via Workspace ONE UEM, comme les analyses, consultez la Déclaration de confidentialité de VMware à l'adresse https://www.vmware.com/help/privacy.html.

Important Les divers pays et juridictions présentent des réglementations différentes régissant les données pouvant être collectées auprès des utilisateurs finaux. Votre organisation doit soigneusement étudier les lois applicables avant de configurer vos stratégies d'utilisation de terminaux personnels et de confidentialité.

Configurer les paramètres de confidentialité

La confidentialité des utilisateurs finaux est notre première préoccupation pour vous et vos utilisateurs. Workspace ONE UEM offre un contrôle granulaire sur les données collectées des utilisateurs et sur les données visibles par les administrateurs. Configurez les paramètres de confidentialité pour répondre aux besoins de vos utilisateurs et à ceux de votre activité.

- Vérifiez et adaptez les politiques de confidentialité en fonction de la propriété du terminal ce qui vous permet de vous conformer aux lois de protection des données en vigueur dans d'autres pays ou aux restrictions légalement définies.

- Assurez-vous que certains rééquilibrages et vérifications informatiques sont en place afin d'empêcher une surcharge des serveurs et des systèmes.

Important chaque territoire a ses propres lois régissant les types de données qui peuvent être recueillies auprès des utilisateurs finaux. Effectuez une recherche détaillée avant de configurer vos politiques de confidentialité.

1 Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Confidentialité**.

2 Sélectionnez les paramètres appropriés pour la collecte des données suivantes : **GPS**, **Télécoms**, **Applications**, **Profils** et **Réseau**.

Collecter et afficher – Les données utilisateur sont collectées et affichées dans UEM Console.

Collecter, ne pas afficher – Les données utilisateur sont collectées pour les rapports, mais ne sont pas affichées dans UEM Console.

Ne pas collecter – Les données utilisateur ne sont pas collectées et, par conséquent, ne sont pas affichées.

3 Sélectionnez le paramètre approprié pour les **commandes** possibles sur les terminaux. Vous pouvez envisager de désactiver toutes les commandes à distance pour les terminaux personnels, en particulier la réinitialisation complète. Ceci empêche l'effacement ou la suppression par inadvertance du contenu personnel d'un utilisateur. si vous désactivez la fonction d'effacement pour certains types de propriété iOS, les utilisateurs ne voient pas l'autorisation « Effacer tous les contenus et paramètres » lors de l'enrôlement.

Autoriser – La commande est effectuée depuis des terminaux sans autorisation de l'utilisateur.

Autoriser cette action avec la permission de l'utilisateur – La commande est exécuté sur les terminaux uniquement si l'utilisateur le permet.

Bloquer – La commande ne s'exécute pas sur les terminaux.

4 Si vous autorisez le contrôle à distance, le gestionnaire de fichiers ou l'accès au gestionnaire du registre pour les terminaux durcis Android/Windows, nous vous conseillons d'utiliser l'option **Autoriser cette action avec la permission de l'utilisateur**. Ce paramètre exige que l'utilisateur final consente à ce que l'administrateur accède à son terminal via une invite avant l'exécution de la commande. Si vous autorisez l'utilisation de toutes les commandes, veillez à le mentionner clairement dans vos conditions d'utilisation.

5 Pour les **informations utilisateur**, indiquez si vous voulez **afficher** ou **ne pas afficher** dans la console les informations relatives au **prénom**, au **nom de famille**, au **numéro de téléphone**, aux **comptes de messagerie** et au **nom d'utilisateur**.

6 Si une option autre que le **nom d'utilisateur** est définie sur **Ne pas afficher**, elle indique alors « Privé » quelles que soient les sections d'UEM Console dans lesquelles elle apparaît. Vous ne pouvez pas rechercher les options définies sur **Ne pas afficher** dans la console. Lorsqu'un nom d'utilisateur est défini sur **Ne pas afficher**, il indique alors « Privé » sur les pages Affichage en liste des terminaux et Détails du terminal seulement. Toutes les autres pages d'UEM Console affichent le nom de l'utilisateur enrôlé.

7 Si vous le souhaitez, vous pouvez chiffrer les informations d'identification personnelles, notamment le prénom, le nom de famille, l'adresse e-mail et le numéro de téléphone. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Sécurité > Sécurité des données** depuis le groupe organisationnel client ou global pour lequel vous souhaitez configurer le chiffrement. Activez le chiffrement, sélectionnez les champs de données utilisateur à chiffrer et cliquez sur **Enregistrer** pour chiffrer les données. En procédant ainsi, vous limiterez certaines fonctionnalités d'UEM Console, comme la recherche, le tri et le filtrage.

8 Sélectionnez si vous souhaitez **Activer** ou **Désactiver** le **Mode Ne pas déranger** sur le terminal. Ce paramètre permet aux utilisateurs d'ignorer les commandes MDM pour une période donnée. Lorsque cette option est activée, vous pouvez sélectionner une période de grâce ou une durée d'activation définie en minutes, heures ou jours à l'issue de laquelle le **Mode Ne pas déranger** expire.

9 **Activez** ou **désactivez** la **déclaration de confidentialité conviviale** sur le terminal.

10 Lorsqu'elle est **activée**, vous pouvez choisir **Oui** (afficher une déclaration de confidentialité) ou **Non** (ne pas afficher de déclaration de confidentialité) pour chaque niveau de propriété : **Personnel**, **Professionnel dédié**, **Professionnel partagé** et **Inconnu**.

11 Cliquez sur **Enregistrer**. La configuration des paramètres de confidentialité étant soumise à restriction, vous devez entrer votre code PIN de console à quatre chiffres pour pouvoir continuer.

Déploiement de la déclaration de confidentialité

Les déclarations de confidentialité sont automatiquement configurées en fonction du groupe organisationnel et du type de propriété du terminal se connectant. Vous pouvez choisir d'afficher une déclaration de confidentialité pour chaque niveau de propriété : **Personnel**, **Professionnel dédié**, **Professionnel partagé** et **Inconnu**.

Lorsque vous attribuez un type de propriété pour recevoir les déclarations de confidentialité, tous les utilisateurs du type de propriété sélectionné reçoivent la notification de confidentialité sous forme de raccourci. Si vous avez inséré la valeur de recherche de la déclaration de confidentialité `PrivacyNotificationUrl` dans votre modèle de message, ce dernier contient alors une URL qui permet à l'utilisateur de lire la déclaration de confidentialité.

Les utilisateurs reçoivent automatiquement la déclaration de confidentialité si :

- ils enrôlent un nouveau terminal et qu'ils appartiennent à un type de propriété pour lequel la déclaration de confidentialité est activée.

- Ils utilisent actuellement un terminal enrôlé et leur type de propriété est modifié après l'enrôlement pour un type qui attribue le raccourci Web.

Pour savoir comment déployer une déclaration de confidentialité lors de l'activation du terminal, consultez la rubrique Inscrire un terminal individuel.

Créer une déclaration de confidentialité pour les utilisateurs BYOD

Informez vos utilisateurs des données collectées sur leurs terminaux enrôlés par votre compagnie à l'aide d'une notification de déclaration de confidentialité. Définissez avec votre service juridique quel message communiquer à vos utilisateurs concernant la collecte des données.

1 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Modèles de message**.

2 Cliquez sur **Ajouter** pour créer un modèle. Si vous avez déjà créé un modèle de notification de déclaration de confidentialité, sélectionnez-le dans la liste de modèles disponibles ou modifiez-le.

3 Complétez les paramètres **Ajouter/Modifier le modèle de message**.

Paramètre	Description
Nom	Saisissez un nom pour le modèle de message.
Description	Saisissez une description du modèle créé.
Catégorie	Cliquez sur **Enrôlement**.
Type	Sélectionnez **Activation du terminal MDM**.
Sélectionner la langue	Sélectionnez la langue par défaut pour votre message. Cliquez sur **Ajouter** pour ajouter plus de langues par défaut pour une distribution multilingue.
Par défaut	Définit ce modèle comme modèle de message par défaut.
Type de message	Sélectionnez un ou plusieurs types de message : **E-mail**, **SMS** ou Message **Push**.

4 Créez une notification de contenu. Les types de message sélectionnés dans **Type de message** décident des messages prêts à être configurés.

Élément	Description
E-mail	
Mise en forme du contenu de l'e-mail	Choisissez entre **Texte brut** ou **HTML** pour votre notification.
Objet	Saisissez l'objet de votre notification.
Corps du message	Rédigez le message de l'e-mail à envoyer à vos utilisateurs. Les outils de modification et de mise en forme qui s'affiche dans la zone de texte dépendent du format choisi dans la **mise en forme du contenu de l'e-mail**. Si vous avez activé la déclaration de confidentialité visuelle, veuillez inclure la valeur de recherche `PrivacyNotificationUrl` dans le corps du message.
SMS	

Élément	Description
Corps du message	Rédigez le message du SMS à envoyer à vos utilisateurs. Si vous avez activé la déclaration de confidentialité visuelle, veuillez inclure la valeur de recherche `PrivacyNotificationUrl` dans le corps de votre message.
Notification Push	
Corps du message	Rédigez le message de la notification Push à envoyer à vos utilisateurs. Si vous avez activé la déclaration de confidentialité visuelle, veuillez inclure la valeur de recherche `PrivacyNotificationUrl` dans le corps de votre message.

5 Cliquez sur **Enregistrer**.

Meilleures pratiques relatives à la confidentialité

Trouver l'équilibre entre vos besoins professionnels et les problèmes de confidentialité de vos employés pose un défi réel. Il existe des méthodes simples pour gérer les paramètres de confidentialité afin de trouver le meilleur équilibre.

Important chaque déploiement est différent. Adaptez au mieux les paramètres et politiques à votre organisation en consultant vos propres équipes juridique, RH et de gestion.

Informations utilisateur pour les meilleures pratiques en matière de confidentialité

En général, vous pouvez afficher les informations sur un utilisateur comme le prénom, le nom de famille, le numéro de téléphone et l'adresse e-mail pour les terminaux personnels et professionnels.

Informations sur l'application pour les meilleures pratiques en matière de confidentialité

En général, il est approprié de définir la collecte des informations sur les applications sur **Ne pas collecter** ou **Collecter, ne pas afficher** pour les terminaux personnels. Ce paramètre est important, car les applications publiques installées sur un terminal peuvent être considérées comme des informations identifiables personnelles si elles sont affichées. Pour les terminaux professionnels, toutes les applications installées sur le terminal seront rapportées à Workspace ONE UEM.

Si l'option « Ne pas collecter » est sélectionnée, seules les informations relatives aux applications personnelles ne seront pas collectées. Workspace ONE UEM collecte toutes les applications gérées, qu'elles soient publiques, internes ou achetées.

Commandes à distance pour les meilleures pratiques en matière de confidentialité

Pensez à désactiver toutes les commandes à distance pour les terminaux personnels. Cependant, si vous souhaitez autoriser les actions ou les commandes à distance, nous vous conseillons de mentionner explicitement ces actions et commandes distantes dans vos conditions d'utilisation.

Collecte de coordonnées GPS pour les meilleures pratiques en matière de confidentialité

La collecte des coordonnées GPS a un lien fondamental avec les préoccupations en matière de protection de la vie privée. Bien que la collecte de données GPS pour les terminaux appartenant à l'employé ne soit pas appropriée, les remarques suivantes s'appliquent à tous les terminaux enrôlés dans Workspace ONE UEM.

- Seul Workspace ONE Intelligent Hub renvoie les données de localisation GPS du terminal à UEM Console.
  - Les autres applications qui utilisent Workspace ONE SDK comme VMware Browser, Content, Boxer, etc. n'envoient pas les données GPS à UEM Console.
  - Le GPS est généralement utilisé pour les terminaux perdus ou volés. Il est également utilisé lorsque l'emplacement d'un terminal fait partie intégrante d'une fonction de Workspace ONE UEM Console, comme les géo-barrières.
  - Lorsque les données GPS sont rapportées, Workspace ONE UEM définit une région d'1 km autour de cet emplacement. Elle rapporte ensuite les informations de localisation lorsque le terminal se situe en dehors de la région.

Données de télécommunications pour les meilleures pratiques

Il est uniquement approprié de collecter les données de télécommunications des terminaux personnels si elles font partie d'une allocation dans le cadre de laquelle vous financez le forfait mobile de l'utilisateur. Dans ce cas, ou pour les terminaux professionnels, les remarques suivantes concernant les données collectées s'appliquent :

- **Opérateur téléphonique/Code pays** – Le code pays et l'opérateur téléphonique sont enregistrés et peuvent être utilisés pour suivre les télécommunications. Les forfaits peuvent être établis et attribués de manière appropriée aux terminaux en fonction de leur opérateur téléphonique et de leur pays. Ces informations peuvent aussi être utilisées pour suivre les terminaux par opérateur téléphonique et pays d'origine ou par opérateur téléphonique et pays actuel.
- **Statut de l'itinérance** – Ce statut peut être utilisé pour suivre les terminaux dont le statut est « En itinérance » ou « Pas en itinérance ». Des politiques de conformité peuvent être définies pour désactiver les appels et les données mobiles en itinérance ou pour effectuer d'autres

actions de conformité. En outre, si un forfait est attribué à un terminal, Workspace ONE UEM peut suivre l'utilisation des données mobiles en itinérance. La collecte et la surveillance du statut d'itinérance peuvent être utiles pour éviter les surcoûts élevés des opérateurs téléphoniques, lors de l'itinérance.

- **Utilisation des données mobiles** – L'utilisation des données mobiles désigne l'utilisation des données en nombre total d'octets envoyés et reçus. Ces données peuvent être collectées pour chaque terminal mobile. Si un forfait est attribué au terminal dans AirWatch, vous pouvez surveiller l'utilisation des données d'après le pourcentage du nombre total de données par cycle de facturation. Cette fonctionnalité vous permet de créer des politiques de conformité basées sur le pourcentage de données utilisées et vous permet d'éviter les surcoûts élevés facturés par les opérateurs téléphoniques.
- **Utilisation des appels** – L'utilisation des appels désigne le nombre de minutes d'appel qui peut être collecté pour chaque terminal mobile. Comme pour l'utilisation des données, si un forfait est attribué au terminal, vous pouvez surveiller l'utilisation d'après le pourcentage de minutes consommées par cycle de facturation. Cette méthode vous permet de créer des politiques de conformité basées sur le pourcentage de minutes utilisées et peut s'avérer utile pour éviter les surcoûts élevés des opérateurs téléphoniques.
- **Utilisation des SMS** – L'utilisation des SMS désigne le nombre de SMS qui peut être collecté pour chaque terminal mobile. Comme pour l'utilisation des données, si un forfait est attribué au terminal, vous pouvez surveiller l'utilisation des SMS d'après le pourcentage du nombre total de messages par cycle de facturation. Cette méthode vous permet de créer des politiques de conformité basées sur le pourcentage de messages utilisés. La surveillance de l'utilisation des SMS permet d'éviter les surcoûts élevés facturés par les opérateurs téléphoniques.

Collecte de données utilisateur auprès des utilisateurs finaux BYOD

L'infrastructure Workspace ONE UEM collecte et stocke de nombreux types de données générées par l'utilisateur. La matrice suivante fait correspondre chaque type de données aux plateformes et aux systèmes d'exploitation à partir desquels les données peuvent être collectées.

Utilisez cette matrice pour déterminer la collecte de données nécessaire à votre déploiement. Workspace ONE UEM définit également des données facultatives que vous pouvez collecter, telles que le MAC Bluetooth. Vous pouvez configurer ces options et attribuer des paramètres de confidentialité par type de propriété : professionnel, partagé et détenu par l'employé.

Pour plus d'informations sur la manière dont VMware traite les données collectées via Workspace ONE UEM, comme les analyses, consultez la Déclaration de confidentialité de VMware à l'adresse https://www.vmware.com/help/privacy.html.

✓ - Peut être collecté.

X - Ne peut pas être collecté.

✓* - Peut être collecté sur des déploiements Workspace ONE Intelligent Hub.

✓** - Peut être collecté sur des déploiements Workspace ONE Intelligent Hub ou iOS 9.3+ mode Supervisé.

	Android	Apple iOS	macOS	Windows durcis	Windows Desktop
Suivi d'application					
Afficher les applications internes installées.	✓	✓	✓	X	✓
Afficher les versions des applications	✓	✓	✓	X	✓
Capturer l'état de l'application	✓	X	✓	X	✓
Certificats					
Afficher la liste des certificats installés	✓	✓	✓	X	✓*
Suivi des actifs					
Nom du terminal	✓	✓	✓	✓	✓
UDID du terminal	✓	✓	✓	✓	✓
Numéro de téléphone	✓	✓	X	✓	✓
Numéro IMEI/MEID	✓	✓	X	✓	✓
Numéro de série du terminal	✓	✓	✓	✓	✓
Numéro IMSI	✓	X	X	✓	✓
Modèle du terminal	✓	✓	✓	✓	X
Nom du modèle de terminal (convivial)	X	✓	✓	✓	X
Fabricant	✓	✓	✓	✓	✓
Version du système d'exploitation	✓	✓	✓	✓	✓
Build du système d'exploitation	✓	X	✓	✓	✓
Version du microprogramme/ noyau	X	X	✓	X	X
Suivi des erreurs du terminal	X	X	✓	✓	✓
État du terminal					
Batterie disponible	✓	✓	✓	✓	✓
Capacité de la batterie	✓	✓	✓	✓	X
Mémoire disponible	✓	✓	✓	✓	X
Capacité de la mémoire	✓	✓	✓	✓	X
Emplacement					
Suivi GPS	✓	✓**	✓	✓	✓

	Android	Apple iOS	macOS	Windows durcis	Windows Desktop
Données Bluetooth	✓	✓**	✓	✓	✓
Données USB	X	✓**	✓	✓	✓
Réseau					
Adresse IP Wi-Fi	✓	✓	✓	✓	✓
MAC Wi-Fi	✓	✓	✓	✓	✓
Force du signal Wi-Fi	X	X	✓	✓	✓
Version des paramètres de l'opérateur	✓	✓	X	X	X
Force du signal mobile	✓	X	X	X	X
Technologie mobile (aucune, GSM, CDMA)	✓	✓	X	X	X
MCC actuel	✓	✓	X	X	X
MNC actuel	✓	✓	X	X	X
Numéro de carte SIM	✓	✓	X	X	✓
Réseau de l'opérateur de la carte SIM	✓	✓	X	X	X
MNC de l'abonné	✓	✓	X	X	X
MAC Bluetooth	✓	✓	✓	X	X
Afficher les adresses IP.	✓	✓	✓	X	X
Afficher les adaptateurs LAN.	X	X	✓	X	X
Afficher l'adresse MAC.	✓	✓	✓	X	X
Itinérance					
Détecter l'état d'itinérance.	✓	✓	X	X	X
Désactiver les notifications Push en itinérance.	X	✓	X	X	X
Itinérance vocale activée (autorisée).	X	✓	X	X	X
Utilisation des données					
Suivi de l'utilisation des données via le réseau mobile	✓	✓	X	X	X
Suivi de l'utilisation des données via un réseau Wi-Fi	X	X	X	X	X
Appels					
Suivi de l'historique des appels	✓	X	X	X	X
Messages					
Suivi de l'historique des SMS	✓	X	X	X	X
État cellulaire					

	Android	Apple iOS	macOS	Windows durcis	Windows Desktop
Réseau de l'opérateur actuel	✓	✓	X	X	X
État actuel du réseau	✓	✓	X	X	X
Affichage à distance					
Terminal de contrôle à distance	✓	X	✓	✓	✓
Capture d'écran (enregistrement, e-mail, impression, etc.)	✓	X	✓	✓	✓
Partage d'écran (vue à distance dans les applications)	✓	✓	X	✓	✓
Gestionnaire de fichiers					
Accès au gestionnaire de fichiers du terminal	✓	X	✓	✓	✓
Accès au gestionnaire de registre du terminal	X	X	X	✓	✓
Copie des fichiers	✓	X	✓	✓	✓
Création de dossiers.	✓	X	✓	✓	✓
Téléchargement de fichiers à partir du terminal.	✓	X	✓	✓	✓
Déplacement de fichier	✓	X	✓	✓	✓
Renommer les dossiers et les fichiers.	✓	X	✓	✓	✓
Télécharger les fichiers vers le terminal	✓	X	✓	✓	✓

Conditions d'utilisation pour les utilisateurs finaux de terminaux personnels

Pour des raisons de responsabilité, vous devez informer les employés des données collectées et des actions autorisées sur les terminaux enrôlés dans Workspace ONE UEM. Pour vous aider à communiquer votre stratégie, créez des accords de Conditions d'utilisation dans Workspace ONE UEM.

Les utilisateurs sont invités à lire et à accepter les conditions d'utilisation que vous configurez avant de pouvoir activer MDM sur leurs terminaux personnels. En attribuant des accords de Conditions d'utilisation en fonction du type de propriété, vous pouvez créer et distribuer des accords différents pour les utilisateurs professionnels et BYOD.

Une fois que votre organisation a écrit son accord de Conditions d'utilisation, envisagez de le communiquer aux utilisateurs finaux dans un livre blanc de une à deux pages n'utilisant pas le jargon juridique. Ce livre blanc ne constitue pas les Conditions d'utilisation officielles acceptées par les utilisateurs finaux, mais sert plutôt à communiquer vos stratégies d'entreprise. Idéalement,

les utilisateurs finaux ne voient pas les conditions d'utilisation des terminaux détenus par les employés lorsqu'ils inscrivent leur terminal pour la première fois. Vous devez être transparents concernant les informations de l'utilisateur final que vous collectez et la manière dont vos stratégies relatives à l'utilisation des terminaux personnels les affectent.

Restrictions pour les terminaux personnels

Workspace ONE UEM vous permet de déployer des stratégies de sécurité et des restrictions différentes pour les terminaux détenus par un employé et les terminaux professionnels.

À l'aide de profils de restriction, vous pouvez définir des restrictions strictes pour les terminaux professionnels et des restrictions plus souples pour les terminaux détenus par un employé. Par exemple, les restrictions à des applications comme YouTube ou les App Store natifs ne sont généralement pas déployées sur des terminaux détenus par des employés. Au lieu de cela, vous pouvez créer des profils de sécurité et des restrictions qui augmentent le niveau de sécurité des terminaux sans avoir un impact négatif sur la fonctionnalité.

Restrictions du terminal agnostique

Workspace ONE UEM rend les restrictions suivantes disponibles pour chaque terminal et plate-forme :

- **Sauvegardes chiffrées** : protégez toutes les sauvegardes avec le chiffrement des données pour les terminaux BYOD ayant accès au contenu de l'entreprise.
- **Forcer l'avertissement de fraude dans les navigateurs pris en charge** : demandez aux utilisateurs d'accuser réception de tous les avertissements émis par le navigateur lorsqu'il détecte un site suspect.
- **Désactiver le déplacement des e-mails** : interdisez l'exposition des données d'entreprise sensibles en désactivant la possibilité de transférer un e-mail d'entreprise vers un compte personnel ou de l'ouvrir dans des applications tierces.

Restrictions spécifiques à la plate-forme

Chaque plate-forme a son propre ensemble de restrictions exécutoires. Évaluez ces restrictions individuellement pour déterminer leur valeur pour votre déploiement. Certaines, comme les restrictions iOS limitées aux terminaux surveillés, ne s'appliquent pas, car les terminaux détenus par un employé ne doivent pas être inscrits avec Apple Configurator.

- Vous pouvez créer des profils de sécurité et des restrictions en accédant à **Ressources > Profils et lignes de base > Profils** et en sélectionnant **Ajouter**, puis en sélectionnant la plateforme appropriée.
- Si vous créez des profils spécifiquement pour des terminaux détenus par un employé, attribuez-les uniquement à des Smart Group en fonction du type de propriété : détenu par l'employé. Pour plus d'informations, consultez la rubrique Smart Groups.

Pour plus d'informations sur la création de profils de sécurité et de restrictions, reportez-vous à la section Ajouter une politique de conformité.

Effacement des données professionnelles pour les terminaux BYOD

Un aspect essentiel de votre déploiement BYOD consiste à supprimer le contenu d'entreprise lorsqu'un employé quitte celle-ci ou lorsqu'un terminal est perdu ou volé. Workspace ONE UEM vous permet d'effectuer un effacement des données professionnelles sur les terminaux pour supprimer tout le contenu d'entreprise et l'accès, tout en conservant les paramètres et les fichiers personnels.

Alors qu'une réinitialisation de terminal rétablit l'état d'usine d'origine d'un terminal, Workspace ONE UEM vous permet de décider du degré d'effacement des données d'entreprise lorsque ce dernier s'applique aux applications VPP publiques et achetées qui se trouvent dans une zone grise entre les terminaux de l'entreprise et les terminaux détenus par l'employé. L'effacement des données professionnelles désenrôle également le terminal de Workspace ONE UEM et supprime tout le contenu activé via MDM qui se trouve sur celui-ci. Cela inclut les comptes de messagerie, les paramètres VPN, les profils Wi-Fi, le contenu sécurisé et les applications d'entreprise.

Si vous avez utilisé des codes d'échange dans le cadre du programme d'achats en grande quantité (VPP) d'Apple pour les terminaux sous iOS 6 et versions antérieures, vous ne pouvez pas récupérer les licences rachetées pour cette application. Une fois installée, l'application est associée au compte App Store de l'utilisateur. Cette association est irréversible. Cependant, vous pouvez échanger des codes de licences utilisés pour iOS 7 et versions ultérieures.

- **Réinitialisation du terminal** – Envoyez une commande MDM pour effacer toutes les données et le système d'exploitation d'un terminal. Cette action est irréversible.
  - Considérations relatives à la réinitialisation de terminal iOS
    - Pour les terminaux iOS 11 et versions antérieures, la commande d'effacement du contenu du terminal efface également les données de la carte SIM Apple associées aux terminaux.
    - Pour les terminaux iOS 11 et versions ultérieures, vous pouvez conserver le forfait de données de la carte SIM Apple (si disponible sur les terminaux). Cochez la case **Conserver le forfait de données** sur la page Effacement du contenu du terminal avant d'envoyer la commande d'effacement du contenu du terminal.

        - Pour les terminaux iOS 11.3 et versions ultérieures, vous disposez d'une option supplémentaire pour ignorer l'écran **Configuration de la proximité** lors de l'envoi de la commande d'effacement du contenu du terminal. Lorsque l'option est activée, l'écran Configuration de la proximité est ignoré dans l'Assistant de configuration, empêchant ainsi l'utilisateur du terminal de voir l'option Configuration de la proximité.
    - Pour les terminaux Windows Desktop, vous pouvez sélectionner le type d'effacement du contenu du terminal.
        - **Effacer** : cette option efface tout le contenu du terminal.
        - **Effacement protégé** : cette option est identique à celle d'effacement normal du contenu du terminal, mais elle ne peut pas être contournée par l'utilisateur final du terminal. La commande d'effacement protégé continue d'essayer de réinitialiser le terminal jusqu'à ce qu'elle réussisse. Dans certaines configurations de terminal, cette commande peut empêcher le terminal de démarrer.
        - **Effacer et conserver les données de provisionnement** : cette option efface le contenu du terminal, mais indique que les données de provisionnement doivent être sauvegardées dans un emplacement permanent. Une fois l'effacement effectué, les données de provisionnement sont restaurées et appliquées au terminal. Le dossier de provisionnement est enregistré. Vous pouvez accéder au dossier en naviguant sur le terminal jusqu'à `%ProgramData%\Microsoft\Provisioning`.
- **Effacement des données professionnelles** – Effacez les données professionnelles du terminal pour le désenrôler et supprimer toutes ses ressources professionnelles gérées, y compris les applications et les profils. Cette action ne peut pas être annulée. De plus, le réenrôlement est nécessaire pour que Workspace ONE UEM gère de nouveau ce terminal. Cette action comprend différentes options pour empêcher un futur réenrôlement et une zone de texte **Description de la note** vous permettant d'ajouter des informations sur l'action.
    - L'effacement des données professionnelles n'est pas pris en charge sur les terminaux joints au domaine Cloud.

Effectuer un effacement des données professionnelles pour un terminal personnel

Un effacement des données professionnelles désenrôle le terminal de Workspace ONE UEM et supprime de tous ses contenus professionnels, y compris les comptes de messagerie, les paramètres de VPN, les profils et les applications.

1 Depuis la Workspace ONE UEM Console, sélectionnez le groupe organisationnel approprié.

2 Accédez à **Terminaux > Affichage en liste** et sélectionnez un ou plusieurs terminaux dans la liste.

3 La vue Détails du terminal affiche une liste d'actions que vous pouvez effectuer sous le menu déroulant **Plus** en haut à droite. Sélectionnez **Effacement des données professionnelles**.

4 Dans la boîte de dialogue de confirmation, sélectionnez **Empêcher la réinscription** pour empêcher ce terminal de s'inscrire de nouveau.

5 Entrez un code PIN de sécurité, le cas échéant, puis sélectionnez **Effacement des données professionnelles** pour terminer l'action.

Désactiver l'effacement complet pour les terminaux personnels

Pour des raisons de sécurité et de confidentialité, vous pouvez désactiver la possibilité d'effectuer un effacement complet sur un terminal personnel.

Si vous désactivez l'effacement complet pour les types de propriété des terminaux iOS sélectionnés, les utilisateurs procédant à l'enrôlement sous ce type de propriété ne verront pas les permissions « Effacer tout le contenu et les paramètres » pendant l'installation du profil.

1 Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Général > Confidentialité**.

2 Faites défiler jusqu'à la section **Commandes** et recherchez la colonne **Propriété de l'employé**.

3 Définissez l'option **Effacement complet** sur **Empêcher** et sélectionnez **Enregistrer**.

Ressources

14

Les ressources de Workspace ONE UEM powered by AirWatch sont semblables à des pièces de puzzle représentant les éléments que vous installez ou configurez sur les terminaux. Les ressources incluent des applications et des livres, des profils, des mises à jour, des capteurs, des scripts, des fenêtres de temps et des ordres d'installation. Une fois regroupées, elles contribuent au fonctionnement sûr et fiable de votre flotte mobile.

Applications et livres

Gérez le catalogue d'applications, le catalogue de livres et les commandes du programme d'achats en volume (VPP). Affichez aussi les données analytiques et les journaux d'applications, ainsi que les paramètres des applications, notamment les catégories d'application, les Smart Groups, les groupes d'applications, les applications recommandées, les géo-barrières et les profils associés aux applications. Pour plus d'informations, reportez-vous à Présentation de la gestion du cycle de vie des applications.

Profils et lignes de base

Profils : les profils des terminaux sont votre principal moyen de gestion des terminaux dans Workspace ONE UEM. Ils représentent des paramètres facilitant l'application des procédures de l'entreprise, lorsqu'ils sont combinés à des politiques de conformité. Pour plus d'informations, reportez-vous à Version d'évaluation technique : profils et ressources de profil utilisés dans les workflows.

Lignes de base : la sécurisation de la configuration de vos terminaux selon les meilleures pratiques est un processus chronophage. Vous pouvez sécuriser tous vos terminaux avec des paramètres et des configurations recommandés par le secteur. Workspace ONE UEM organise ces meilleures pratiques dans des configurations appelées lignes de base. Ces configurations réduisent considérablement le temps nécessaire à l'installation et à la configuration des terminaux Windows. Pour plus d'informations, reportez-vous à la section Utilisation des lignes de base.

Mises à jour du terminal

Gérez tous les fichiers de mise à jour de votre terminal, y compris l'historique complet des états d'installation de chaque mise à jour, dans un seul emplacement. La fonctionnalité Mises à jour du terminal est propre à la plateforme. Pour plus d'informations, consultez les guides de plateforme pour Windows Desktop, Android et iOS.

Capteurs

Les capteurs sont un type spécial de script. Un script est une commande programmable exécutée à la demande.

Un capteur est également programmable, mais il est principalement utilisé comme une condition programmable. Le nom du capteur devient la clé, dont la valeur provient de l'exécution d'actions basées sur des déclencheurs externes, comme une action d'agent, une planification ou un événement. L'action peut également être exécutée à la demande. Les clés de capteur et les valeurs résultantes sont ensuite utilisées comme conditions pour les attributions.

Pour plus d'informations, reportez-vous à Création de capteurs pour les terminaux Windows Desktop et Capteurs pour les terminaux macOS.

Scripts

Un script est une ressource programmable qui est exécutée pour collecter des valeurs ou affecter une modification au terminal. Les scripts sont déclenchés sur le terminal par des conditions de capteur, exécutés à la demande ou au cours d'un workflow Freestyle.

Pour plus d'informations, reportez-vous à Scripts pour Windows Desktop et Scripts pour les terminaux macOS.

Fenêtre de temps

La mise à jour de terminaux avec du contenu provisionné et d'autres contenus téléchargeables peut être un processus long. La fonctionnalité de fenêtre de temps vous permet de planifier ces téléchargements en dehors des heures de travail principales, en utilisant l'heure locale du terminal. Vous n'avez plus besoin de choisir entre la mise à jour de votre terminal et la productivité.

Pour plus d'informations, reportez-vous à Version d'évaluation technique : créer une fenêtre de temps et l'appliquer aux terminaux.

Commandes

Les commandes font référence au contenu acheté via le programme d'achats en volume (VPP) d'Apple Business Manager et à la distribution de ce contenu à l'aide de codes de rachat et de la distribution gérée. Pour plus d'informations sur les commandes et le programme VPP, reportez-vous à Programme d'achats en volume dans le Guide d'Apple Business Manager.

Ce chapitre contient les rubriques suivantes :

- Version d'évaluation technique : créer une fenêtre de temps et l'appliquer aux terminaux

Version d'évaluation technique : créer une fenêtre de temps et l'appliquer aux terminaux

Les fenêtres de temps vous permettent de planifier les mises à jour et la diffusion du contenu Workspace ONE UEM en tenant compte de vos heures d'activité et de maintenance. Réglez votre fenêtre de temps en planifiant les dates de début et de fin, la durée et les options de répétition.

Actuellement, les fenêtres de temps ne sont prises en charge que par les terminaux Windows Desktop.

Si vous disposez déjà d'une fenêtre de temps définie et que vous souhaitez l'utiliser, passez directement à l'étape 2 pour l'attribuer.

Note Workspace ONE UEM offre la fonctionnalité de fenêtre de temps sous la forme d'une version d'évaluation technique. Les fonctionnalités de la version d'évaluation technique ne sont pas entièrement testées et certaines peuvent ne pas fonctionner comme prévu. Cependant, ces versions d'évaluation technique permettent à Workspace ONE UEM d'améliorer les fonctionnalités actuelles et de développer de futures améliorations. Pour utiliser une fonctionnalité de version d'évaluation technique, contactez votre représentant VMware.

Conditions préalables

Avant que vous puissiez afficher, créer ou attribuer une fenêtre de temps, votre compte d'administrateur doit avoir un rôle qui inclut les autorisations de rôle pour ces activités. Pour plus d'informations, reportez-vous à la section Rôles administrateur.

Chemin d'accès à la catégorie d'autorisation	Nom de l'autorisation
Gestion des terminaux > Fenêtre de temps	Gérer la fenêtre de temps (créer, modifier et attribuer)
	Afficher la fenêtre de temps
	Afficher la fenêtre de temps sur la page Détails du terminal

Procédure

1 Créer une fenêtre de temps.

   a Accédez à **Ressources > Fenêtres de temps** et sélectionnez le bouton **Nouvelle**.

   b Renseignez les options **Nom**, **Description**, **Catégorie** et **Temps**.

   Catégorie : vous pouvez créer une fenêtre de temps dédiée aux heures de maintenance et une fenêtre de temps distincte pour les heures ouvrées, ce qui vous permet de concevoir un planning adapté à chaque catégorie. Cette façon de procéder peut être utile dans les environnements à haute disponibilité et à trafic élevé.

   Heure : vous pouvez sélectionner la période sur laquelle votre fenêtre de temps est basée. Si vos mises à jour dépendent fortement de la distinction entre les heures ouvrées et non ouvrées, vous pouvez utiliser l'heure du terminal pour la fenêtre de temps. Cependant, si une mise à jour doit être synchronisée sur tous les terminaux indépendamment de l'heure locale, vous pouvez sélectionner UTC pour cette fenêtre de temps spécifique.

   c Renseignez les options **Répéter**, **Date de début**, **Date de fin** et **Durée**. La durée minimale est de 1 heure.

   Vous pouvez ajouter plus d'une planification par fenêtre de temps définie en sélectionnant le bouton **Ajouter une planification**, puis en créant un autre ensemble de sélections **Répéter**, **Date de début**, **Date de fin** et **Durée**.

   Les raisons de définir plusieurs planifications par fenêtre de temps peuvent varier : vous pouvez avoir plusieurs pics d'activité dans vos heures de maintenance, vous pouvez avoir plusieurs creux dans vos heures de travail, et ainsi de suite.

   Lorsque plusieurs planifications existent, vous pouvez supprimer une planification spécifique en sélectionnant l'icône de corbeille dans le coin supérieur droit de la fenêtre.

   d Finalisez la fenêtre de temps.

   - **Enregistrer** : enregistrez la fenêtre de temps sans l'attribuer.
   - **Enregistrer et attribuer** : enregistrez et attribuez immédiatement la fenêtre de temps.

2 Attribuez une fenêtre de temps aux terminaux.

   a Accédez à **Ressources > Fenêtre de temps**. L'affichage en liste des fenêtres de temps s'affiche.

   b Localisez la fenêtre de temps que vous souhaitez appliquer à votre terminal et sélectionnez-la en cliquant sur le bouton radio à gauche de son entrée dans la liste.

   c Sélectionnez le bouton **Attribuer** qui s'affiche au-dessus de la liste.

   L'écran Attributions s'affiche.

d Attribuer la fenêtre de temps à un Smart Group à l'aide de la barre de recherche **Smart Groups**. Pour plus d'informations, consultez la section Créer un Smart Group. Gardez à l'esprit que les fenêtres de temps ne fonctionnent actuellement que sur les terminaux Windows Desktop. Dans tout Smart Group sélectionné ici comprenant des terminaux qui ne sont pas du type Windows Desktop, la fenêtre de temps ne sera pas attribuée à ces terminaux.

e Une fois que vous avez sélectionné un Smart Group dans la barre de recherche **Smart Groups**, cliquez sur le bouton **Attribuer** pour terminer cette étape.

f Utiliser la fenêtre de temps dans une condition de workflow. Suivez les étapes indiquées dans la rubrique Créer un workflow avec une condition de fenêtre de temps.

Étape suivante

Suivez la fenêtre de temps d'un terminal en affichant la **vue Détails** de ce terminal. Pour cela, accédez à **Détails > Affichage en liste** et sélectionnez un terminal spécifique dans la liste. Pour plus d'informations, reportez-vous à Chapitre 8 Détails du terminal.

Vous pouvez inviter les utilisateurs à sélectionner **Synchroniser le terminal** depuis l'application Workspace ONE Intelligent Hub afin de mettre à jour l'état de synchronisation indiqué dans la **vue Détails**.

Les événements de la fenêtre de temps sont consignés par l'enregistreur des événements lorsque le niveau de journalisation minimal est défini sur **Information** ou **Débogage**. Pour plus d'informations, consultez le documentJournaux des événements.

Terminaux partagés

15

La fonctionnalité de terminaux partagés/multi-utilisateurs de Workspace ONE UEM 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, 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 iPads Apple intégrés à Apple Business Manager. Cette fonctionnalité appelée iPads 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 iPads partagés pour les entreprises avec Apple Business Manager et comment obtenir cette fonctionnalité, reportez-vous à la section **iPads 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.

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.

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 Cliquez sur **Enregistrer**.

Se connecter et se déconnecter des terminaux macOS partagés

Plusieurs utilisateurs peuvent se connecter à un terminal macOS partagé et s'en déconnecter en activant le transfert automatique des profils de terminaux.

Se connecter à un terminal macOS : à l'aide des informations d'identification attribuées pour le réseau, connectez-vous à un terminal macOS préenrôlé et vous recevrez les profils attribués à votre compte dans Workspace ONE UEM.

Se déconnecter d'un terminal macOS : la procédure de déconnexion macOS standard déconnecte également le terminal du profil utilisateur Workspace ONE UEM qui vous est attribué.

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.

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.

Que faire ensuite ? Pour vous déconnecter d'un terminal Android, sélectionnez **Paramètres de Launcher**, puis **Déconnexion** (icône de la porte).

Se connecter et se déconnecter des terminaux iOS partagés

Vous pouvez vous connecter à un terminal iOS partagé par plusieurs utilisateurs et vous en déconnecter.

1 Exécutez Workspace ONE Intelligent Hub sur le terminal.

2 Saisissez les identifiants de l'utilisateur.

Si le terminal est déjà connecté à Workspace ONE Intelligent Hub, les utilisateurs sont invités à saisir un code d'accès SSO. Si le terminal n'est pas connecté, les utilisateurs sont invités à saisir un nom d'utilisateur et un mot de passe. Les profils attribués à chaque utilisateur sont déployés en fonction du Smart Group et des associations de groupes d'utilisateurs.

Note si l'option **Demander à l'utilisateur de saisir le groupe organisationnel** est activée, l'utilisateur doit saisir un **ID de groupe** pour ouvrir une session sur un terminal.

3 Sélectionnez **Connexion** et acceptez les **Conditions d'utilisation**.

Note s'ils sont invités à fournir un code d'accès, les utilisateurs peuvent en créer un dans le portail en libre-service. Ces codes d'accès ont une date d'expiration. À l'approche de cette date d'expiration, Workspace ONE Intelligent Hub invite les utilisateurs à changer leur code d'accès sur le terminal. Si les utilisateurs ne changent pas leur code d'accès avant son expiration, ils doivent retourner sur le portail en libre-service pour en créer un autre.

Que faire ensuite ? Pour vous déconnecter d'un terminal iOS, exécutez Workspace ONE Intelligent Hub et sélectionnez **Déconnexion** en bas.

Faire le check-in d'un terminal partagé à partir d'UEM Console

Vous pouvez faire le check-in d'un terminal directement depuis Workspace ONE UEM Console, évitant ainsi à l'utilisateur final de le faire à l'aide de l'instance de Workspace ONE Intelligent Hub installée.

Lorsque vous faites le check-in d'un terminal à l'aide d'UEM Console, vous réinitialisez efficacement l'enrôlement sur le préenrôlement de plusieurs utilisateurs avec le groupe organisationnel, les profils, les applications, etc. prescrits. Côté terminal, Workspace ONE Intelligent Hub est redémarré, et l'écran de check-out s'affiche.

Cette fonction ne s'applique actuellement qu'aux terminaux iOS. Les terminaux enrôlés à l'aide d'une autre méthode que Workspace ONE Intelligent Hub (par exemple, l'enrôlement direct, Workspace ONE ou AirWatch Container) ne sont pas pris en charge. Le check-in de terminaux en masse depuis la console n'est pas pris en charge.

1 Accédez à **Terminaux > Affichage en liste** et localisez le terminal iOS partagé dont vous voulez faire le check-in.

2 Sélectionnez le **nom convivial** du terminal pour afficher ses **détails**.

3 Cliquez sur le bouton **Plus d'actions** dans le coin supérieur droit de l'écran.

4 Dans la section **Gestion**, sélectionnez **Faire le check-in du terminal**.

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.

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.

Paramètre	Description
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.
Conserver le code d'accès d'un terminal partagé pendant au moins (jours)	Définissez la durée minimale (en jours) durant laquelle le code d'accès au terminal partagé devra être modifié.
Inviter les utilisateurs à changer le code d'accès de leurs terminaux partagés x (jours) avant son expiration	**(Pour terminaux iOS uniquement)** Définissez, en nombre de jours avant l'expiration, le moment où l'utilisateur reçoit un rappel lui indiquant de changer son code d'accès au terminal partagé. Pour de meilleurs résultats, définissez une valeur inférieure à la différence entre l'heure d'expiration et la durée minimale pendant laquelle vous pouvez conserver le code secret de terminal partagé.
historique du code d'accès	Définissez le nombre de codes d'accès enregistrés dans le système afin de renforcer la sécurité de l'environnement en évitant que l'utilisateur ne réutilise un ancien code d'accès.
Déconnexion automatique	Configurez la déconnexion automatique après une période définie.
Déconnexion automatique après	Définissez le laps de temps avant l'activation de la fonction de **déconnexion automatique** en **minutes**, **heures** ou **jours**.
Mode Application unique iOS	Cochez cette case pour configurer le mode application unique, qui verrouille le terminal dans une application unique lorsqu'un utilisateur s'y connecte. Pour exporter un terminal iOS en mode d'application unique, les utilisateurs se connectent à l'aide de leurs identifiants. Lorsque le terminal est de nouveau importé, il repasse en mode d'application unique. L'activation du mode Application unique désactive également le bouton d'accueil sur le terminal. **Note** Le mode d'application unique ne s'applique qu'aux terminaux iOS supervisés.

4 Configurez les **Paramètres de déconnexion**, le cas échéant.

Paramètre	Description
Effacez les données d'application Android	Effacez les données d'application lorsque l'utilisateur se déconnecte d'un terminal partagé (check in).
Réinstaller des applications Android	Utilisez le menu déroulant pour choisir de toujours réinstaller l'application entre les utilisateurs ou de ne jamais réinstaller l'application entre les utilisateurs. Pour les déploiements Android (hérité), vous pouvez choisir de réinstaller l'application si le hub ne peut pas effacer les données d'application entre les utilisateurs.
Effacer le code secret Android du terminal	Ce paramètre permet de contrôler que le code secret actuel du terminal Android est effacé lorsque l'utilisateur se déconnecte (connexion) d'un terminal partagé par plusieurs utilisateurs.

Paramètre	Description
Autoriser le code PIN au démarrage	Activez ou désactivez le démarrage sécurisé Android, qui nécessite d'entrer un code PIN la première fois pour démarrer le terminal. Si l'option est désactivée, 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, celui-ci doit être réinitialisé aux paramètres d'usine pour l'activer. Cette fonctionnalité s'applique uniquement aux périphériques 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**.

Que faire ensuite ? 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 des terminaux à utilisateur unique et Préenrôler des terminaux partagés.

Protection contre la réinitialisation 16

Vous pouvez vous protéger contre les effacements de terminaux excessifs et les effacements d'entreprise en définissant un seuil d'effacement dans Workspace ONE UEM.

L'effacement distant d'un contenu professionnel d'un terminal, appelé Effacement des données professionnelles, est l'une des mesures envisagées en cas de perte ou de vol d'un terminal. Cette fonction fait office de protection contre la menace de voir le contenu d'entreprise exposé à la concurrence. Un effacement de terminal est potentiellement plus destructeur, car il supprime tout le contenu et remet le terminal à son état d'origine.

- **Réinitialisation du terminal** – Envoyez une commande MDM pour effacer toutes les données et le système d'exploitation d'un terminal. Cette action est irréversible.
  - Considérations relatives à la réinitialisation de terminal iOS
    - Pour les terminaux iOS 11 et versions antérieures, la commande d'effacement du contenu du terminal efface également les données de la carte SIM Apple associées aux terminaux.
    - Pour les terminaux iOS 11 et versions ultérieures, vous pouvez conserver le forfait de données de la carte SIM Apple (si disponible sur les terminaux). Cochez la case **Conserver le forfait de données** sur la page Effacement du contenu du terminal avant d'envoyer la commande d'effacement du contenu du terminal.
    - Pour les terminaux iOS 11.3 et versions ultérieures, vous disposez d'une option supplémentaire pour ignorer l'écran **Configuration de la proximité** lors de l'envoi de la commande d'effacement du contenu du terminal. Lorsque l'option est activée, l'écran Configuration de la proximité est ignoré dans l'Assistant de configuration, empêchant ainsi l'utilisateur du terminal de voir l'option Configuration de la proximité.
  - Pour les terminaux Windows Desktop, vous pouvez sélectionner le type d'effacement du contenu du terminal.
    - **Effacer** : cette option efface tout le contenu du terminal.
    - **Effacement protégé** : cette option est identique à celle d'effacement normal du contenu du terminal, mais elle ne peut pas être contournée par l'utilisateur final du terminal. La commande d'effacement protégé continue d'essayer de réinitialiser le terminal jusqu'à ce qu'elle réussisse. Dans certaines configurations de terminal, cette commande peut empêcher le terminal de démarrer.

- **Effacer et conserver les données de provisionnement** : cette option efface le contenu du terminal, mais indique que les données de provisionnement doivent être sauvegardées dans un emplacement permanent. Une fois l'effacement effectué, les données de provisionnement sont restaurées et appliquées au terminal. Le dossier de provisionnement est enregistré. Vous pouvez accéder au dossier en naviguant sur le terminal jusqu'à `%ProgramData%\Microsoft\Provisioning`.

- **Effacement des données professionnelles** – Effacez les données professionnelles du terminal pour le désenrôler et supprimer toutes ses ressources professionnelles gérées, y compris les applications et les profils. Cette action ne peut pas être annulée. De plus, le réenrôlement est nécessaire pour que Workspace ONE UEM gère de nouveau ce terminal. Cette action comprend différentes options pour empêcher un futur réenrôlement et une zone de texte **Description de la note** vous permettant d'ajouter des informations sur l'action.
  - L'effacement des données professionnelles n'est pas pris en charge sur les terminaux joints au domaine Cloud.

Cependant, il existe des circonstances dans lesquelles des processus planifiés tels que le moteur de conformité et d'autres directives automatisées réinitialisent plusieurs terminaux. En plus des effacements automatisés, un effacement accidentel lancé par un administrateur peut être problématique. En tant qu'administrateur, vous devez savoir lorsqu'une telle action est initiée et pouvoir intervenir.

Configurez les paramètres de protection contre la réinitialisation en définissant un seuil d'effacement, c'est-à-dire le nombre minimum de terminaux réinitialisés en un certain lapse de temps. Par exemple, si plus de 10 terminaux sont effacés en 20 minutes, vous pouvez automatiquement placer les effacements à venir en attente jusqu'à ce que vous ayez validé les commandes d'effacement.

Vous pouvez vérifier les journaux des réinitialisations pour savoir quand et pour quelle raison les terminaux ont été réinitialisés. Une fois la vérification des informations effectuée, vous pouvez accepter ou refuser les commandes de réinitialisation mises en attente et déverrouiller le système afin de remettre le seuil à zéro.

Configurer les paramètres de protection contre la réinitialisation sur les terminaux gérés

Définissez un seuil de réinitialisation pour les terminaux gérés et informez les administrateurs par e-mail lorsque ce seuil est atteint. Vous pouvez configurer ces paramètres pour les groupes organisationnels de type « global » ou « client » seulement.

1 Accédez à **Terminaux > Cycle de vie > Paramètres > Protection contre la réinitialisation**.

2 Configurez les paramètres suivants.

Paramètre	Description
Terminaux réinitialisés	Saisissez le nombre de **terminaux réinitialisés** qui servent de seuil pour déclencher la protection contre l'effacement.
En (minutes)	Saisissez une valeur dans le champ **En (minutes)** définissant le laps de temps au cours duquel les réinitialisations doivent avoir lieu pour déclencher la protection contre la réinitialisation.
E-mail	Sélectionnez un modèle de message à envoyer aux administrateurs. Créez un modèle de message pour la protection contre l'effacement en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Modèles de message**, puis sélectionnez **Ajouter**. Ensuite, cliquez sur Suivant, sélectionnez **Cycle de vie du terminal** comme **Catégorie** et **Notification de protection contre l'effacement** comme **Type**. Vous pouvez utiliser les valeurs de recherche suivantes dans votre modèle de message. ■ {EnterpriseWipeInterval} – Valeur apparaissant dans le champ **En (minutes)** sur la page des paramètres. ■ {WipeLogConsolePage} – Lien vers la page de journaux des réinitialisations.
à	Entrez les adresses e-mail des administrateurs qui doivent être notifiés. Ces derniers doivent avoir accès à la page Journaux d'effacement.

Pour plus d'informations, reportez-vous à la section Chapitre 12 Valeurs de recherche.

3 Cliquez sur **Enregistrer**.

Afficher les journaux des effacements

Vous pouvez vérifier la page des **journaux des effacements** pour savoir quand et pour quelle raison les terminaux ont été effacés. Une fois la vérification des informations effectuée, vous pouvez accepter ou refuser les commandes d'effacement mises en attente et déverrouiller le système afin de réinitialiser le décompte du seuil des terminaux.

Si le système est verrouillé, un bandeau apparaîtra en haut de la page pour l'indiquer.

1 Accédez à **Terminaux > Cycle de vie > Journal des effacements**.

L'accès à cette page est géré par la ressource **Rapporter les journaux d'effacement du terminal** et est disponible par défaut pour les administrateurs système, les administrateurs SaaS et les administrateurs Workspace ONE UEM. Vous pouvez l'ajouter à n'importe quel rôle administrateur personnalisé depuis la page **Créer un rôle admin**.

2 **Filtrez** le journal des effacements en suivant ces paramètres. Les choix sont les suivants :

- Plage de dates
- Type d'effacement
- État
- Source
- Propriété

3 Affichez la liste des terminaux et déterminez s'il s'agit d'effacements valides ou non.

Les actions en attente sur les terminaux afficheront le statut « En attente ». Les terminaux réinitialisés avant que la limite ne soit atteinte apparaîtront comme « traités ».

a Dans le cas de réinitialisations valides, sélectionnez chaque terminal, puis cliquez sur **Approuver le(s) effacement(s)** dans la liste de commandes. Le statut apparaîtra alors comme Approuvé.

b Dans le cas de réinitialisations non valides, sélectionnez chaque terminal puis cliquez sur **Rejeter le(s) effacement(s)** dans la liste de commandes. Le statut apparaîtra alors comme Rejeté.

4 Réinitialisez le compteur du seuil de terminaux et autorisez l'exécution des commandes d'effacement en sélectionnant **Déverrouiller le système**.

Le système permet des commandes d'effacement automatisées futures jusqu'à ce que la limite du seuil soit à nouveau dépassée. Cette action est possible pour les groupes organisationnels de type « global » ou « client » seulement.