Documentation Windows Desktop

VMware Workspace ONE UEM 2306

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

Gestion des terminaux Workspace ONE UEM, conditions requises en matière d'enrôlement et systèmes d'exploitation Windows pris en charge 11

- Workspace ONE UEM prend en charge Windows 11 11
- Gestion des terminaux Workspace ONE UEM pour les terminaux Windows 11
- Conditions d'enrôlement requises pour les terminaux Windows 11
  - Conditions requises côté utilisateur 12
  - Conditions requises côté terminal 13
- Quelles sont les versions de systèmes d'exploitation Windows prises en charge ? 14
- Matrice de la version de Windows 14

Enrôlement de terminaux Windows dans Workspace ONE UEM 17

- Notions de base relatives à l'enrôlement 17
- Enrôlement de Workspace ONE Intelligent Hub pour Windows 18
  - Procédure d'enrôlement à VMware Workspace ONE Intelligent Hub 19
- Enrôlement MDM natif pour Windows Desktop 19
  - Enrôlement par l'intermédiaire de Work Access avec Windows Auto Discovery 20
  - Enrôlement par l'intermédiaire de Work Access sans Windows Auto Discovery 22
- Préenrôlement des terminaux Windows 24
  - Importer par lots des numéros de série de terminal 24
  - Carbon Black et Workspace ONE Intelligent Hub pour Windows 25
    - Où se trouvent les paramètres Carbon Black ? 26
  - Enrôlement par préenrôlement à l'aide de la ligne de commande 26
  - Enrôlement par l'intermédiaire du préenrôlement manuel d'un terminal 27
  - Paramètres et valeurs de l'enrôlement silencieux 28
    - Paramètres généraux 28
    - Paramètres Enrôlement pour le compte d'un utilisateur 29
    - Paramètres Carbon Black 29
  - Exemples d'enrôlement silencieux 30
- Intégration de Workspace ONE UEM et Azure AD 31
  - Environnements SaaS : Azure AD en tant que service d'identité 31
  - Environnements sur site ou environnement SaaS avec un nom de domaine personnalisé : Azure AD en tant que service d'identité 33
  - Enrôler un terminal avec Azure AD 35
  - Enrôler un terminal Azure AD géré dans Workspace ONE UEM 35

Enrôlement en mode OOBE (Out-of-Box Experience) 36

Enrôlement via les applications Office 365 39

Provisionnement et enrôlement par lots pour les terminaux Windows 40

Enrôlement avec le provisionnement par lots 40

Installer des packages de provisionnement 42

Enrôlement avec le Mode Enregistré 42

Paramètres d'intégration après enrôlement 43

Critères à prendre en compte 43

Comportements du VMware Workspace ONE Intelligent Hub 43

Désactiver l'expérience d'intégration après l'enrôlement 43

Personnaliser le message d'expérience d'intégration après l'enrôlement 44

États d'enrôlement Windows 44

Enrôlement de terminaux pour la prise en charge multi-utilisateurs : Phase 1 (2210+) 47

Présentation des fonctionnalités 47

Exigences relatives à la version d'évaluation technique 47

Enrôlement de systèmes multi-utilisateurs 49

Flux d'enrôlement 49

Attributions de ressources 54

FAQ 54

Profils Workspace ONE UEM pour Windows 55

Que sont les profils 55

Niveau de l'utilisateur ou du terminal 55

Nouvelles options de profil pour la configuration des profils d'utilisateurs et de terminaux Windows 57

Option de plateforme Windows 58

Option de plateforme Windows(bêta) 58

Indicateur de fonctionnalité - Modèles VMware 59

Profil d'antivirus 60

Profil de contrôle d’applications 62

Configuration d'un profil Contrôle des applications 63

Profil BIOS 64

Profil Identifiants 68

Configuration d'un profil Identifiants 69

Profil des paramètres personnalisés 71

Protection contre la désactivation par les utilisateurs du service Workspace ONE UEM 72

Profil Dynamic Environment Manager (DEM) 73

Documentation DEM 73

- CDN requis 73
- Critères à prendre en compte 73
- Tâches à effectuer avant l'intégration 74
- Configuration d'un profil DEM 75
- Application des modifications du profil de configuration DEM 75

Profil Protection des données 75
- Configuration d'un profil Protection des données 77
- Création d'un certificat de système de fichiers chiffré 79

Profil Defender Exploit Guard 80
- Windows Defender Exploit Guard 80
- Exploit Protection 80
- Réduction de la surface d'attaque 80
- Accès contrôlé aux dossiers 80
- Protection réseau 81
- Informations supplémentaires 81
- Création d'un profil Defender Exploit Guard 81

Profil Chiffrement 83
- Fonctionnalité BitLocker 83
- Comportement du déploiement 84
- États de chiffrement 84
- Clés de récupération 85
- Comportement de suppression 85
- BitLocker et stratégies de conformité 85
- Prise en charge de BitLocker To Go 86
  - Où trouver les informations de la clé de récupération ? 86
- Interrompre BitLocker dans la console 87
- Configurer un profil Chiffrement 87

Profil Exchange ActiveSync 91
- Suppression de profils ou effacement des données d'entreprise 91
- Nom d'utilisateur et mot de passe 91
- Configuration d'un profil Exchange ActiveSync 91

Profil Services Web Exchange 93

Profil Pare-feu 93

Profil Pare-feu (Hérité) 96

Profil de kiosque 98

Profil de mises à jour OEM 100

Profil de mot de passe 102

Profil Peer Distribution 104
- Configuration d'un profil Distribution pair à pair 105

Profil de personnalisation 106
Profil Proxy 107
Profil Restrictions 107
Profil SCEP 112
Configuration d'un profil SCEP 112
Profil Mode d'application unique 113
Profil VPN 114
VPN par application pour Windows utilisant le profil VPN 118
Profil Raccourcis Internet 119
Profil Wi-Fi 120
Profil Windows Hello 121
Création d'un profil Windows Hello 122
Profil Gestion des licences Windows 123
Profil Mises à jour Windows 123
Dépannage concernant les mises à jour de fonctionnalités et de qualité 126
Profil de mises à jour Windows (héritées) 126
Mises à jour des terminaux pour Windows Desktop 130
Application gérée sur le profil poste de travail Windows 131
Navigation 131
Onglet Windows 131
Onglet des mises à jour OEM 131

Utilisation des Lignes de base 133
Micro-service Cloud 133
Les Lignes de base nécessitent une connectivité constante aux services du terminal 133
Types de Lignes de base 133
Considérations relatives à l'évaluation CIS 134
Attribution de lignes de base 134
Gestion des Lignes de base 134
Exemple de copie d'une ligne de base 135
Réappliquer des lignes de base 136
État de conformité des Lignes de base 137
Interrogation des états de conformité des lignes de base 137
Vérification de l'état de conformité 137
Création d'une ligne de base 138
Conditions prérequises 138
Création de lignes de base avec un modèle 138
Création de lignes de base personnalisées 140

politiques de conformité 141
Stratégies de conformité dans Workspace ONE UEM 141
Dell BIOS Verification pour Workspace ONE UEM 141
Avantages de Dell Trusted Device 141
Préparer vos terminaux à Dell Trusted Device 142
États de Dell BIOS Verification 142
Détection des terminaux compromis avec attestation d'intégrité 142
Configurer les politiques de conformité d'attestation d'intégrité pour Windows Desktop 143

Applications Windows Desktop 147
Applications de productivité Workspace ONE 147
Application VMware Workspace ONE pour Windows Desktop 147
Configurer Workspace ONE Intelligent Hub pour Windows Desktop 147
Ajout d'applications Win32 et gestion 148
Différer l’installation de l’application dans UEM 148

Collecter des données avec des Capteurs pour les terminaux Windows Desktop 150
Fonctionnalité Freestyle 150
Description des Capteurs 150
Options Workspace ONE UEM 151
Déclencheurs de capteurs 151
Ajout de scripts PowerShell 151
Détails du terminal > Capteurs 151
Options Workspace ONE Intelligence 152
Rapports et tableaux de bord pour analyser les données 152
RBAC pour contrôler l'accès aux données 152
Chiffrement 152
Utiliser Write-Ouput et Not Write-Host dans les scripts 152
Exemple de script non opérationnel 152
Exemple de script opérationnel 152
Documentation de Workspace ONE Intelligence 153
Terminaux Windows Desktop et données des capteurs 153
Exemples de scripts PowerShell pour les Capteurs 153
Vérifier le niveau de batterie restant 153
Obtention du numéro de série 153
Obtention de la date système 153
Vérification de l'activation du TPM 154
Vérification du verrouillage du TPM 154
Obtention de l'heure de correction du TPM verrouillé 154

Vérification de la présence du SMBIOS 154
Vérification de la version BIOS de SMBIOS 154
Affichage de la version du BIOS 154
Affichage de l'état du BIOS 155
Affichage de l'utilisation moyenne du CPU (%) 155
Affichage de l'utilisation moyenne de la mémoire 155
Affichage de l'utilisation moyenne de la mémoire virtuelle 155
Affichage de l'utilisation moyenne du réseau 155
Affichage de l'utilisation moyenne de la mémoire pour un processus 156
Vérification de l'exécution ou de la non-exécution d'un processus 156
Vérification de l'activation du démarrage sécurisé 156
Interface réseau active 156
Vérification de la version de PowerShell 156
Vérification de la capacité maximale de la batterie 157
Vérification de l'état de charge de la batterie 157
Profil de gestion de l'alimentation actif 157
Vérification de la présence d'un réseau sans fil 157
Obtention de la version Java 158
Créer un capteur pour les terminaux Windows Desktop 158

Automatiser les configurations de point de terminaison à l'aide de scripts pour les terminaux Windows Desktop 161
Fonctionnalité Freestyle 161
Description des Scripts 161
Comment savoir si vos Scripts s'exécutent avec succès ? 161
Créer un script pour les terminaux Windows Desktop 162

Dell Command | Product Integrations 165
Dell Command | Configure 165
Dell Command | Monitor 165
État d'intégrité de la batterie 165
Dell Command | Update 165
Configurer Dell Command | Products dans Workspace ONE UEM 166

Gestion de terminaux Windows Desktop 167
Tableau de bord des terminaux 167
Affichage en liste des terminaux 169
Personnalisez l'aperçu de l'affichage en liste des terminaux 170
Exporter l'affichage en liste 170
Recherche dans l'affichage en liste des terminaux 170

Cluster de boutons d'action d'affichage en liste du terminal 171
Assistance à distance 171
Détails de la page Terminal Windows Desktop 171
Détails du service de notification Windows 172
Plus d'actions 173
Gérer vos terminaux Microsoft HoloLens 176
Enrôlement de vos terminaux HoloLens 176
Gérer vos terminaux HoloLens 176
Gérer et enrôler vos terminaux Arm64 176
Provisionnement de produit 177
Gestion des mises à jour Windows Device 177
Tableau de bord des mises à jour 178
Dépannage concernant les mises à jour de fonctionnalités et de qualité 178

Déploiement de configurations de jonction de domaine pour Windows 180
Intégration à Microsoft Autopilot (jonction de domaine hybride) 180
Utiliser un profil Windows Autopilot pour les enrôlements OOBE 180
Configurations requises 180
Conditions 181
Ordre des tâches 181
Première étape : Configurer les terminaux Autopilot 182
Deuxième étape : Configurer la jonction de domaine sur site 182
Jonction de domaine sur site 182
Configurations requises 182
Conditions 183
Ordre des tâches 183
Première étape : Configurer ADUC 183
Deuxième étape : Configurer ACC 185
Troisième étape : Créer une jonction de domaine sur site 186
Quatrième étape : Attribuer une configuration de jonction de domaine 187
Conteneur d'ordinateurs dans les conflits OU/Smart Groups et Active Directory (AD) 187
Réattribution de jonction de domaine 187
Joindre un groupe de travail 187
Ordre des tâches 188
Première étape : Créer une jonction de domaine pour les groupes de travail 188
Deuxième étape : Attribuer une configuration de jonction de domaine 188

Intégration d'Intel vPro Endpoint Management Assistant (EMA) de disponibilité générale pour Windows on SaaS 190
Conditions prérequises 190

Configurer l'intégration Intel EMA 190

Déploiement de la configuration des groupes de points de terminaison Intel EMA et de l'agent à l'aide des déploiements d'applications UEM 191

Procédure 191

Rechercher les détails du module de groupe de points de terminaison dans la console 194

Exécuter les opérations gérées par Intel EMA sur les terminaux gérés depuis la console 195

Conditions prérequises 195

Procédure 196

Comportements des opérations Intel EMA 196

Liens officiels de téléchargement Intel 196

Gestion des terminaux Workspace ONE UEM, conditions requises en matière d'enrôlement et systèmes d'exploitation Windows pris en charge

Workspace ONE UEM fournit un ensemble de solutions de gestion de la mobilité pour inscrire, sécuriser, configurer et gérer les déploiements de terminaux Windows. Pour utiliser les solutions de gestion de Workspace ONE UEM, respectez les conditions requises pour enrôler les terminaux Windows pris en charge. La disponibilité de la solution de gestion dépend de la version de système d'exploitation Windows de vos terminaux.

Workspace ONE UEM prend en charge Windows 11

Workspace ONE UEM prend en charge les terminaux Windows 11. Lors de la configuration de la console, utilisez l'option **Windows Desktop**, car cette option fonctionne pour les terminaux Windows 10 et Windows 11. Windows 11 repose sur les mêmes bases que Windows 10. Par conséquent, les fonctionnalités de Workspace ONE UEM disponibles pour Windows 10 sont également disponibles pour Windows 11. Si vous trouvez une fonctionnalité de Workspace ONE UEM qui fonctionne sur Windows 10, mais pas sur Windows 11, contactez VMware Global Services.

Pour plus d'informations sur Windows 11, reportez-vous à la documentation de Microsoft sur les Nouveautés de Windows.

Gestion des terminaux Workspace ONE UEM pour les terminaux Windows

Workspace ONE UEM Console vous propose plusieurs outils et fonctionnalités pour gérer le cycle de vie complet des terminaux de l'entreprise et des employés. Vous pouvez également permettre aux utilisateurs d'accomplir eux-mêmes certaines tâches grâce au portail self-service et à l'auto-enrôlement, ce qui vous permet de gagner des ressources et un temps précieux.

Workspace ONE UEM vous permet d'enrôler des terminaux de l'entreprise et des employés afin de configurer et de sécuriser les données et le contenu de l'entreprise. Nos profils de terminaux vous aideront à configurer et sécuriser correctement vos terminaux Windows. Détectez les terminaux compromis et supprimez leur accès aux ressources de l'entreprise à l'aide du moteur de conformité.

Le fait d'enrôler vos terminaux dans Workspace ONE UEM permet de garantir leur sécurité et de les configurer en fonction des besoins de votre entreprise.

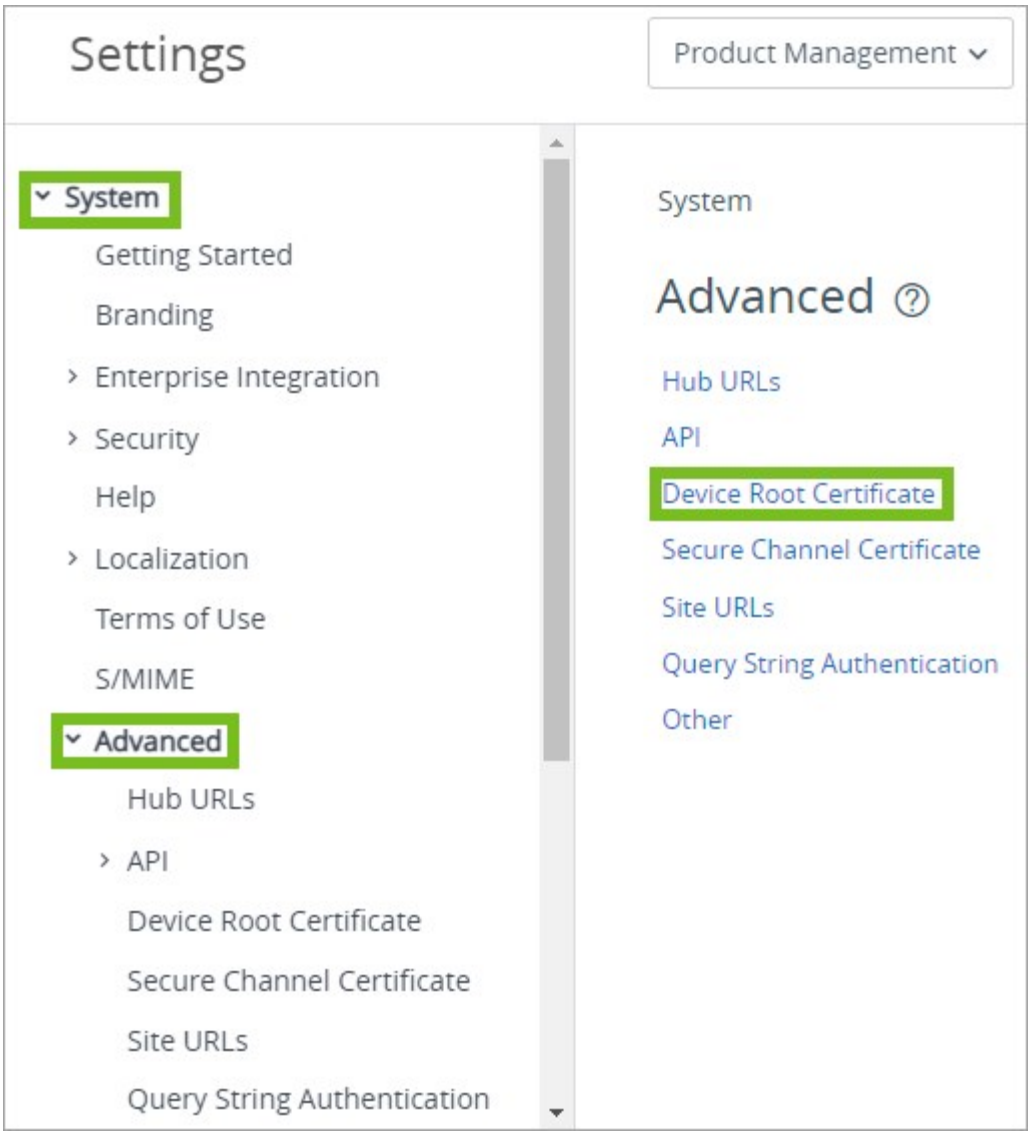
Conditions d'enrôlement requises pour les terminaux Windows

Avant d'enrôler vos terminaux Windows avec Workspace ONE UEM, vos terminaux et utilisateurs finaux doivent répondre aux exigences et configurations répertoriées, autrement l'enrôlement ne fonctionne pas.

Conditions requises côté utilisateur

Vos utilisateurs Windows doivent répondre à cette liste de conditions requises pour enrôler leurs terminaux avec Workspace ONE UEM.

- **Autorisations d'administrateur** : l'utilisateur connecté qui enrôle le terminal doit être un administrateur.
- **ID de groupe** : si votre environnement Workspace ONE UEM demande aux utilisateurs leur ID de groupe, l'utilisateur connecté a besoin de cette valeur.
- **Certificat racine du terminal** : tous les utilisateurs doivent configurer le certificat racine du terminal dans les paramètres système avant d'enrôler de leurs terminaux. Pour configurer le certificat, accédez à **Groupes et paramètres** > **Tous les paramètres** > **Système** > **Avancé** > **Certificat racine du terminal**.



- **URL d'enrôlement :** tous les utilisateurs peuvent saisir une URL unique qui les dirige directement vers l'écran d'enrôlement pour s'enrôler dans un environnement Workspace ONE UEM. Par exemple, **mdm.example.com**.
  Important : Si le serveur d'enrôlement se trouve derrière un proxy, vous devez configurer les services WINHTTP pour qu'ils soient informés de l'existence de ce proxy lors de la configuration de vos paramètres réseau.

Conditions requises côté terminal

Vos terminaux Windows doivent accéder aux sites répertoriés, activer les paramètres répertoriés et disposer des services répertoriés en cours d'exécution pour s'enrôler dans Workspace ONE UEM.

- **URL d'accès** : approuvez ces URL dans vos stratégies de pare-feu pour que vos terminaux enrôlés puissent y accéder.
  - **URL de l'API d'App Center** : permettent à Workspace ONE Intelligent Hub pour Windows de fournir des informations sur le blocage à Microsoft Store.
    - `api.appcenter.ms`
    - `api.mobile.azure.com`
  - **URL de l'API Microsoft Store** : permet à VMware Workspace ONE Intelligent Hub

pour Windows de se lancer sur vos terminaux Windows, quel que soit le marché Microsoft Store sur lequel vos terminaux sont utilisés.
Si vous souhaitez obtenir des informations sur Microsoft Store et les applications prises en charge pour chaque marché, consultez l'article Définir la sélection du marché.

- `http://licensing.mp.microsoft.com/v7.0/licenses/contentHTTPSUsed`

- **Exécution de PowerShell** : activez l'exécution de PowerShell sur vos terminaux Windows, car Workspace ONE UEM utilise PowerShell pour l'installation et les modifications opérationnelles via VMware Workspace ONE Intelligent Hub.
- **Windows Services** : vos terminaux Windows doivent disposer des services répertoriés dans un **État de service : en cours d'exécution** pour vous permettre de vous enrôler et de travailler dans votre déploiement Workspace ONE UEM.
  - DmEnrollmentSvc (service d'enrôlement de la gestion des terminaux)
  - DiagTrack (expériences utilisateur connectées et télémétrie)
  - Schedule (planificateur de tâches)
  - BITS (Background Intelligent Transfer Service)
  - dmwappushservice (Device Management Wireless Application Protocol (WAP) Push message Routing Service)

Quelles sont les versions de systèmes d'exploitation Windows prises en charge ?

Workspace ONE UEM prend en charge l'enrôlement et la gestion des terminaux Windows. Le niveau de prise en charge dépend de la version du système d'exploitation et de l'architecture du terminal.

Workspace ONE UEM prend en charge les terminaux exécutant les systèmes d'exploitation suivants :

- Windows Pro
- Windows Entreprise
- Windows Éducation
- Windows Famille
- Windows S

Workspace ONE Intelligent Hub ne prend pas en charge les terminaux Windows ARM Snapdragon ou Hololens. Ces terminaux doivent utiliser une fonctionnalité MDM native.

Important : pour afficher la version du système d'exploitation que prend en charge chaque branche de mise à jour, consultez la documentation de Microsoft sur les informations de version de Windows : Santé de la version de Windows.

Matrice de la version de Windows

Comparez la fonctionnalité MDM dans chaque version du système d'exploitation Windows. Workspace ONE UEM prend en charge toutes les versions du système d'exploitation Windows, ainsi

que les fonctions prises en charge.

Les différentes éditions de Windows (Famille, Professionnel, Entreprise et Éducation) sont dotées de fonctionnalités différentes. L'édition Windows Famille ne prend pas en charge les fonctionnalités avancées disponibles dans le système d'exploitation Windows. Envisagez d'utiliser les éditions Entreprise ou Éducation pour bénéficier de la plupart des fonctionnalités.

Fonctionnalité	Système d'exploitation Windows Famille	Système d'exploitation Windows Professionnel	Système d'exploitation Windows Entreprise	Système d'exploitation Windows Éducation
Enrôlement client natif	✓	✓	✓	✓
Enrôlement basé sur agent	✓	✓	✓	✓
Nécessite un ID de compte Windows				
Acceptation obligatoire du CLUF/des conditions d'utilisation	✓	✓	✓	✓
Prise en charge des demandes d'option lors de l'enrôlement	✓	✓	✓	✓
Active Directory/LDAP	✓	✓	✓	✓
Enrôlement par jonction à un domaine Cloud		✓	✓	✓
Enrôlement immédiat		✓	✓	✓
Enrôlement par provisionnement par lots		✓	✓	✓
Préenrôlement d'un terminal	✓	✓	✓	✓
SMS				
E-mails		✓	✓	✓
Politique de mot de passe	✓	✓	✓	✓
Effacement des données professionnelles	✓	✓	✓	✓
Réinitialisation complète du terminal	✓	✓	✓	✓
E-mail et Exchange ActiveSync	✓	✓	✓	✓
Wi-Fi	✓	✓	✓	✓
VPN	✓	✓	✓	✓

Fonctionnalité	Système d'exploitation Windows Famille	Système d'exploitation Windows Professionnel	Système d'exploitation Windows Entreprise	Système d'exploitation Windows Éducation
Gestion des certificats	✓	✓	✓	✓
Restrictions et gestion du terminal	✓	✓	✓	✓
Windows Hello	✓	✓	✓	✓
Personnalisation			✓	✓
Chiffrement		✓	✓	✓
Contrôle des applications (AppLocker)			✓	✓
Attestation d'intégrité	✓	✓	✓	✓
Windows Update for Business		✓	✓	✓
Accès attribué			✓	✓
Gestion d'applications		✓	✓	✓
Suivi des actifs		✓	✓	✓
Statut des terminaux		✓	✓	✓
Adresse IP				
Emplacement	✓	✓	✓	✓
Réseau		✓	✓	✓
Envoi de messages au support technique (E-mails et SMS uniquement)		✓	✓	✓

Enrôlement de terminaux Windows dans Workspace ONE UEM

Workspace ONE UEM prend en charge différentes méthodes pour enrôler vos terminaux Windows. Découvrez quel workflow d'enrôlement répond le mieux à vos besoins en fonction de votre déploiement Workspace ONE UEM, des intégrations d'entreprise et du système d'exploitation du terminal.

Notions de base relatives à l'enrôlement

Simplifiez vos enrôlements d'utilisateurs finaux en configurant Windows Auto-Discovery Services (WADS) au sein de votre environnement Workspace ONE UEM. WADS prend en charge une solution sur site et dans le Cloud des services WADS.

Les méthodes d'enrôlement font appel à la fonctionnalité native MDM du système d'exploitation Windows, à Workspace ONE Intelligent Hub pour Windows ou à l'intégration d'Azure AD.

- Enrôlement de Workspace ONE Intelligent Hub pour Windows

  Le workflow d'enrôlement le plus simple utilise Workspace ONE Intelligent Hub pour Windows pour enrôler des terminaux. Les utilisateurs ont juste à télécharger VMware Workspace ONE Intelligent Hub sur getwsone.com et à suivre les invites d'enrôlement à l'écran.

  Envisagez d'utiliser Workspace ONE Intelligent Hub pour le workflow d'enrôlement de Windows. Workspace ONE UEM prend en charge des workflows d'enrôlement supplémentaires pour certains cas d'utilisation spécifiques.

- Enrôlement via une intégration d'Azure AD

  Par le biais de l'intégration avec Microsoft Azure Active Directory (AD), les terminaux Windows s'enrôlent automatiquement dans Workspace ONE UEM avec une interaction minime de la part de l'utilisateur. L'enrôlement via l'intégration d'Azure AD simplifie l'enrôlement des utilisateurs et des administrateurs. L'enrôlement de l'intégration Azure AD prend en charge trois flux d'enrôlement différents : Devenir membre Azure AD, prendre un abonnement Out of Box Experience et prendre un abonnement Office 365. Toutes les méthodes nécessitent la configuration de l'intégration d'Azure AD à Workspace ONE UEM.

  Pour pouvoir enrôler vos terminaux à l'aide de l'intégration d'Azure AD, vous devez configurer Workspace ONE UEM et Azure AD.

- Enrôlement MDM natif

  Workspace ONE UEM prend en charge l'enrôlement des terminaux Windows Desktop à l'aide du flux de travail d'enrôlement MDM. Le nom de la solution MDM native fluctue en fonction de la version de Windows. Le flux d'enrôlement varie en fonction de la version de

Windows et de l'utilisation, ou non, des services WADS.

Seuls les utilisateurs dotés d'autorisations administrateur local sur le terminal peuvent enrôler ce dernier dans Workspace ONE UEM et activer MDM.

- Préenrôlement d'un terminal

  Pour configurer la gestion des terminaux sur un terminal Windows avant de le livrer à votre utilisateur final, il est conseillé d'utiliser le préenrôlement via Windows Desktop. Ce workflow d'enrôlement vous permet en effet d'enrôler un terminal via Workspace ONE Intelligent Hub, d'installer des profils au niveau du terminal, puis de le livrer à l'utilisateur. Il existe deux méthodes de préenrôlement : une installation manuelle et une installation via une ligne de commande. L'installation manuelle exige que les terminaux soient joints au domaine par l'intermédiaire d'Azure AD. L'installation via une ligne de commande fonctionne pour tous les terminaux Windows.

- Enrôlement automatique de terminaux Windows Desktop

  Workspace ONE UEM prend en charge l'enrôlement automatique des terminaux Windows Desktop spécifiques achetés chez Dell. L'enrôlement automatique simplifie le processus d'enrôlement en enrôlant automatiquement les terminaux enregistrés après l'expérience immédiate.

  Windows Provisioning Service by VMware s'applique uniquement aux terminaux Dell Enterprise dotés de la bonne image Windows. La fonctionnalité d'enrôlement automatique doit être achetée dans le cadre de la commande d'achat chez Dell.

- Déploiement et enrôlement par lots

  Le provisionnement par lots permet de créer un package préconfiguré qui préenrôle les terminaux Windows, puis les enrôle dans Workspace ONE UEM. Le provisionnement par lots exige d'importer le kit Microsoft Assessment and Development Kit et d'installer l'outil ICD (Imaging and Configuration Designer). Cet outil crée des packages de provisionnement utilisés pour créer des images des terminaux.

  Grâce à ces flux de provisionnement par lots, vous pouvez utiliser des paramètres Workspace ONE UEM dans le package de provisionnement de sorte que les terminaux provisionnés soient enrôlés automatiquement lors de la première utilisation immédiate.

- Mode Enregistré : enrôlement sans gestion des terminaux

  Pour permettre à certains terminaux Windows de s'enrôler dans Workspace ONE UEM sans les services de gestion des terminaux, vous pouvez activer le mode Enregistré. Attribuez ce mode à l'intégralité d'un groupe organisationnel ou à des Smart Group.

Enrôlement de Workspace ONE Intelligent Hub pour Windows

Workspace ONE Intelligent Hub propose une ressource unique pour l'enrôlement et facilite la communication entre le terminal et Workspace ONE UEM console. Utilisez VMware Workspace ONE Intelligent Hub pour enrôler vos terminaux Windows. Workspace ONE Intelligent Hub fournit aux utilisateurs un workflow d'enrôlement simple et rapide.

Envisagez d'utiliser Workspace ONE Intelligent Hub pour Windows pour enrôler vos terminaux Windows Desktop, car il fournit le workflow d'enrôlement le plus simple pour les utilisateurs. Si vous

avez configuré Workspace ONE, le téléchargement de Workspace ONE Intelligent Hub depuis https://getwsone.com/ télécharge également l'application Workspace ONE. Lorsque vous terminez l'enrôlement auprès de Workspace ONE Intelligent Hub, l'application Workspace ONE se lance et se configure automatiquement en fonction de votre déploiement Workspace ONE UEM.

Workspace ONE Intelligent Hub offre une fonctionnalité supplémentaire à vos terminaux Windows Desktop, y compris les services de localisation.

Vous pouvez simplifier l'enrôlement pour vos utilisateurs à l'aide de Windows Auto-Discovery. Windows Auto-Discovery permet aux utilisateurs de saisir leur adresse e-mail pour remplir automatiquement les zones de texte avec leurs identifiants d'enrôlement.

AirWatch Cloud Messaging (AWCM) permet la livraison en temps réel de stratégies et de commandes à Workspace ONE Intelligent Hub. Sans AWCM, la livraison de stratégies et de commandes à Workspace ONE Intelligent Hub se fait uniquement aux intervalles normaux de check-in définis dans Workspace ONE UEM console. Envisagez d'utiliser AWCM pour distribuer en temps réel des politiques et des commandes aux terminaux Windows Desktop.

Procédure d'enrôlement à VMware Workspace ONE Intelligent Hub

1. Accédez à https://getwsone.com sur le terminal Windows Desktop.
2. Installez VMware Workspace ONE Intelligent Hub. Lorsque l'installation est terminée, démarrez Workspace ONE Intelligent Hub.
3. Saisissez l'adresse e-mail et sélectionnez **Suivant**.
4. Si vous n'utilisez pas la détection automatique pour Windows, définissez les paramètres suivants.
    1. Saisissez l'**URL du serveur** et sélectionnez **Suivant**.
    2. Saisissez l'**ID de groupe** et sélectionnez **Suivant**.
    3. Saisissez le **nom d'utilisateur** et le **mot de passe**.
5. **Acceptez** les conditions d'utilisation.
6. Sélectionnez **Terminé**.
7. Ouvrez Workspace ONE Intelligent Hub et terminez l'enrôlement.

Enrôlement MDM natif pour Windows Desktop

Toutes les méthodes d'inscription de Windows Desktop utilisent le client MDM natif Accès professionnel. Utilisez l'enrôlement de client MDM natif pour enrôler des terminaux d'entreprise et personnels (BYOD) à l'aide du même processus d'enrôlement. Vous pouvez vous enrôler avec ou sans la détection automatique pour Windows.

Work Access commence par traiter un workflow Azure AD pour les domaines connectés à Office 365 ou Azure AD lorsque vous sélectionnez **Connecter** et ne termine pas le workflow d'enrôlement automatiquement. Si vous utilisez Office 365 ou Azure AD sans licence Premium, utilisez VMware Workspace ONE Intelligent Hub pour enrôler les terminaux Windows à la place de l'enrôlement MDM natif. Pour effectuer le workflow d'enrôlement à l'aide de l'enrôlement MDM natif, sélectionnez **Connecter** deux fois. Si vous avez une licence Premium Azure AD, vous pouvez activer **Gestion requise** dans votre instance Azure pour que l'enrôlement MDM natif effectue le flux

d'enrôlement après le flux de travail Azure. Vous pouvez utiliser l'enrôlement MDM natif sans problème si vous n'utilisez pas Office 365 ou Azure AD.

Seuls les utilisateurs dotés d'autorisation administrateur local sur le terminal peuvent enrôler un terminal dans Workspace ONE UEM et activer MDM. Les autorisations Administrateur de domaine ne fonctionnent pas pour l'enrôlement d'un terminal. Pour enrôler un terminal avec un utilisateur standard, utilisez la méthode de configuration par lots pour les terminaux Windows.

Le service Windows Auto-Discovery simplifie l'enrôlement pour les utilisateurs en réduisant leur interaction nécessaire lors du processus.

Les terminaux joints à un domaine peuvent être enrôlés à l'aide de la méthode d'enrôlement Espace de travail native. L'adresse e-mail entrée dans les paramètres est remplie automatiquement à l'aide de l'attribut UPN Active Directory. Si l'utilisateur souhaite utiliser une autre adresse e-mail, il doit télécharger la mise à jour facultative.

Enrôlement par l'intermédiaire de Work Access avec Windows Auto Discovery

Work Access est la méthode d'enrôlement MDM native pour les terminaux Windows. L'enrôlement par Work Access et avec Windows Auto Discovery fournit aux utilisateurs un flux d'enrôlement simple et rapide.

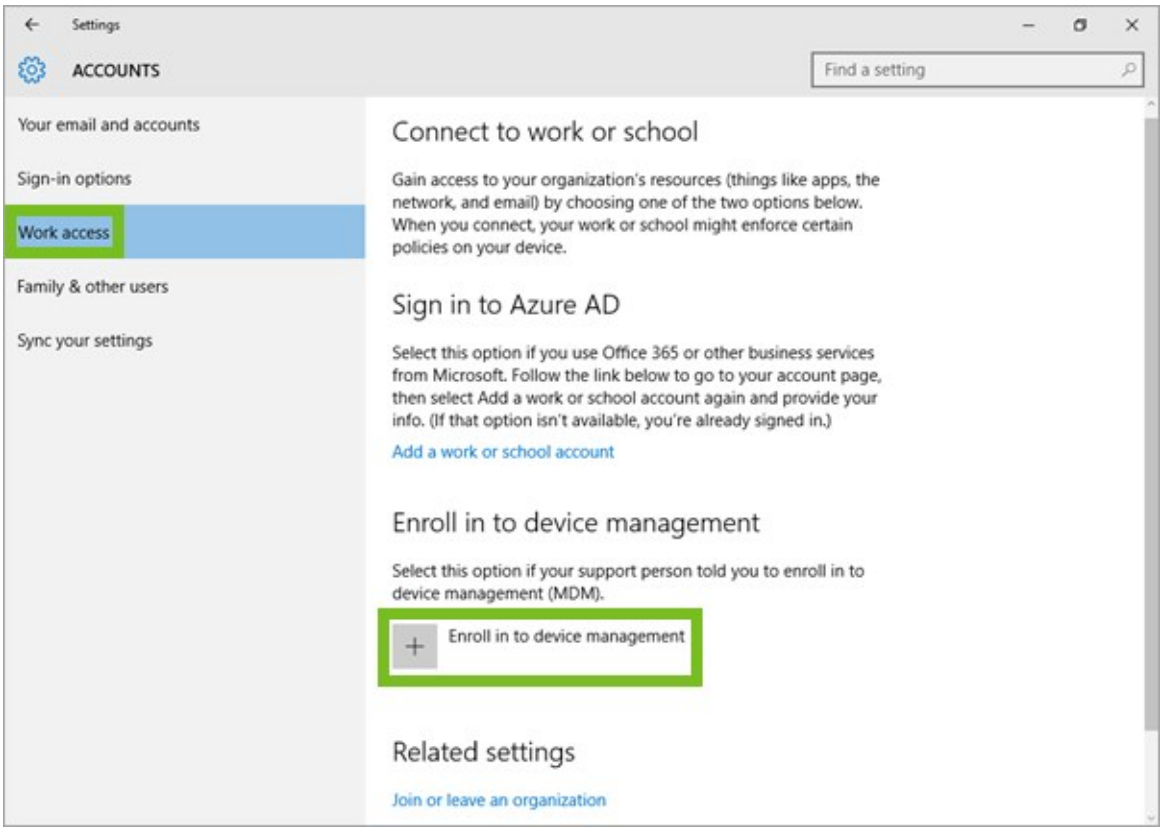
Conditions prérequises

L'enregistrement de votre domaine dans Workspace ONE UEM évite d'avoir à entrer l'ID de groupe au cours de l'enrôlement.

Remarque : Envisagez d'utiliser VMware Workspace ONE Intelligent Hub pour Windows pour enrôler vos terminaux Windows au lieu d'utiliser l'enrôlement MDM natif. Le flux d'enrôlement MDM natif n'enrôle pas les terminaux dans MDM si vous utilisez Office 365 ou Azure AD sur le même domaine.

Procédure

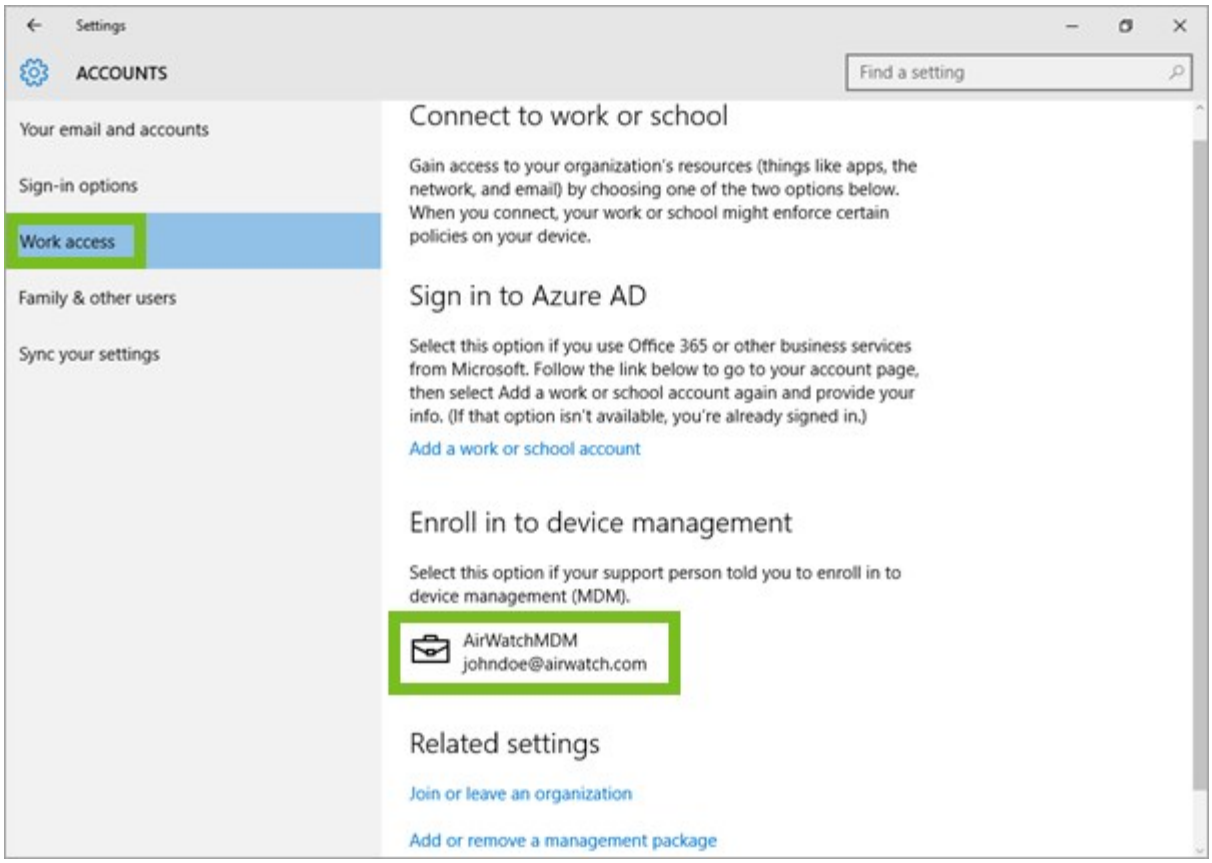
1. Sur le terminal de l'utilisateur, accédez à **Paramètres** > **Comptes** > **Accès professionnel** et sélectionnez **Enrôler dans la gestion des terminaux**.



2. Dans la zone de texte **E-mail**, saisissez le nom d'utilisateur fourni à votre utilisateur suivi du domaine de l'environnement au format `Username@domain.com` (par exemple `jdoe1@acme.com`). Sélectionnez **Continuer**.
3. Saisissez l'**ID de groupe** et sélectionnez **Suivant**.
4. Saisissez le **Nom d'utilisateur** et le **Mot de passe**, puis sélectionnez **Suivant**. Il peut s'agir de vos identifiants de services d'annuaire ou d'identifiants dédiés propres à votre environnement Workspace ONE UEM.
5. **Facultatif** : Lisez le Contrat de licence d'utilisateur final et sélectionnez **J'accepte** pour accepter les conditions d'utilisation.
6. **Facultatif** : Sélectionnez **Oui** pour enregistrer vos informations de connexion.

Résultats

Le terminal tente alors de se connecter à Workspace ONE UEM. Si la connexion réussit, une icône en forme de mallette sur laquelle est inscrit Workspace ONE UEM, apparaît. Cette icône indique que vous avez réussi à vous connecter à Workspace ONE UEM.



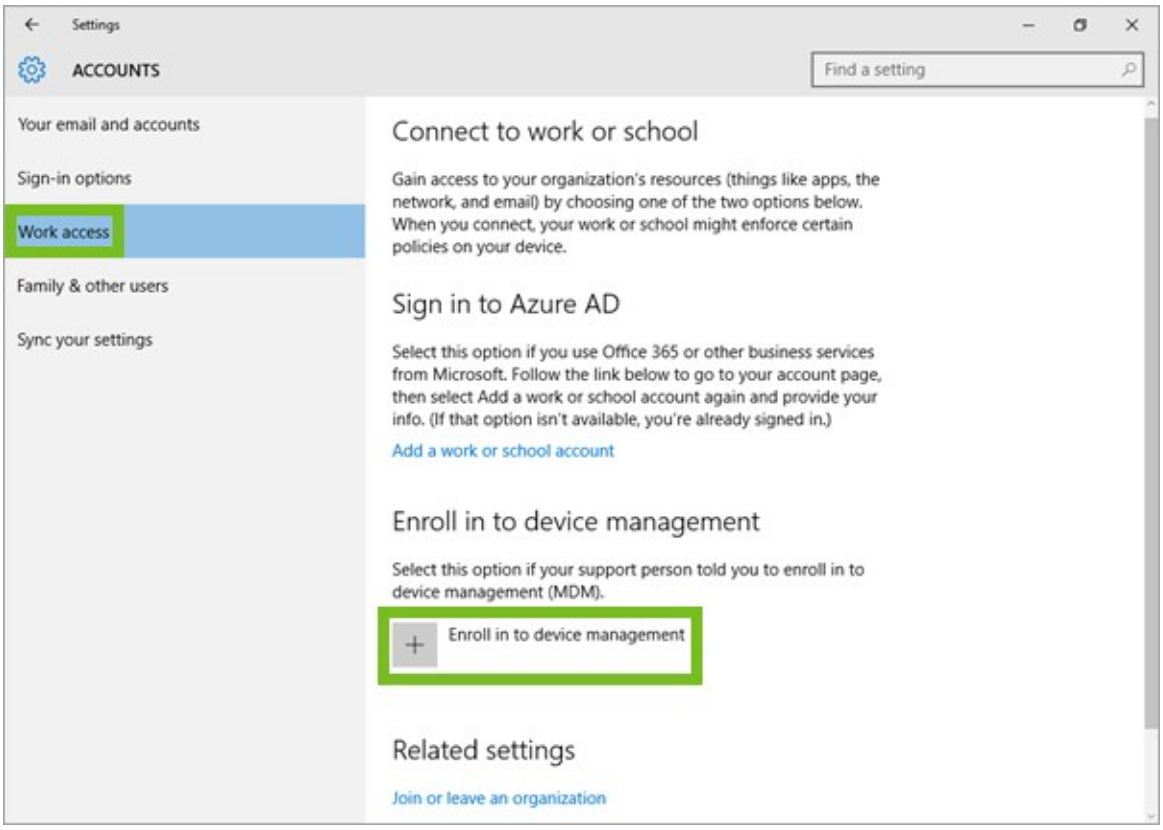
Enrôlement par l'intermédiaire de Work Access sans Windows Auto Discovery

Work Access est la méthode d'enrôlement MDM native pour les terminaux Windows. L'enrôlement via Work Access sans WADS nécessite la saisie manuelle des identifiants de l'utilisateur.

Envisagez d'utiliser VMware Workspace ONE Intelligent Hub pour Windows pour enrôler vos terminaux Windows au lieu d'utiliser l'enrôlement MDM natif. Le flux d'enrôlement MDM natif n'enrôle pas les terminaux dans MDM si vous utilisez Office 365 ou Azure AD sur le même domaine.

Procédure

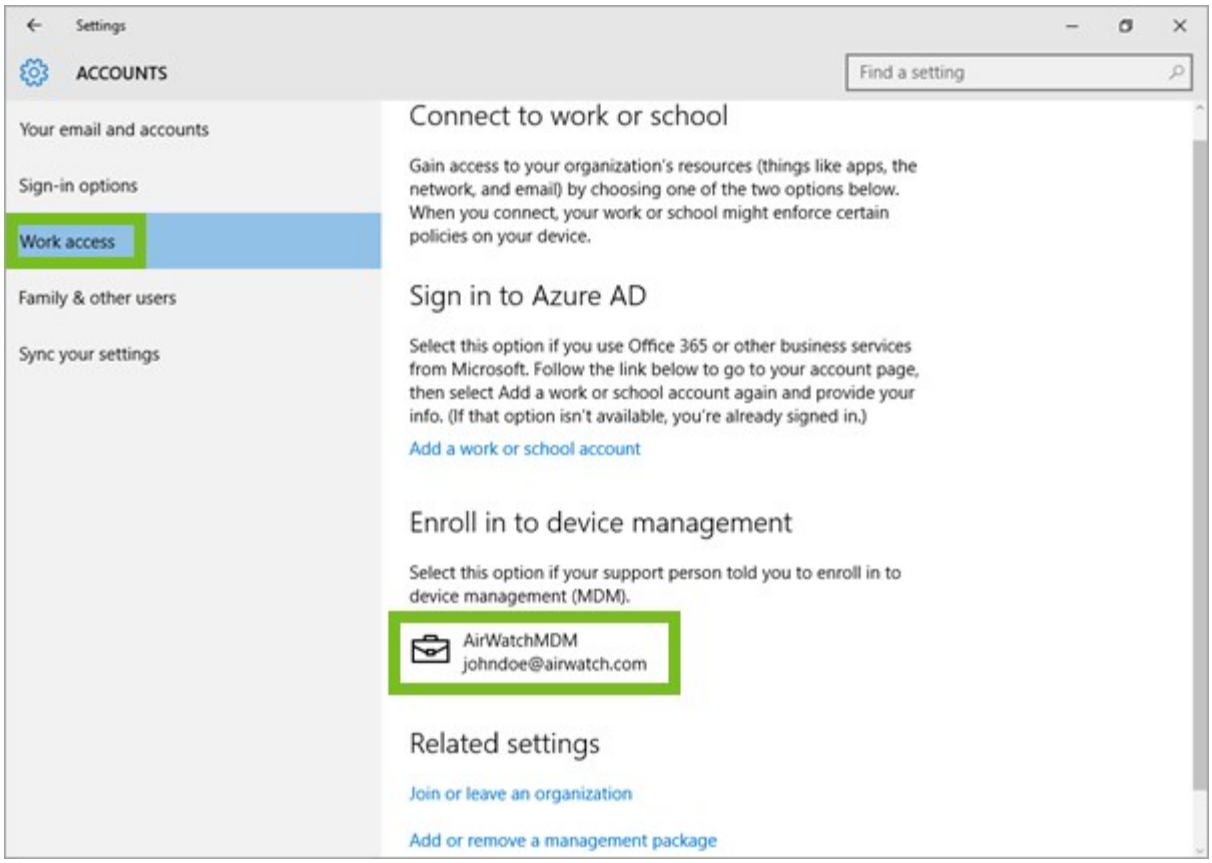
1. Sur le terminal de l'utilisateur, accédez à **Paramètres** > **Comptes** > **Accès professionnel** et sélectionnez **Enrôler dans la gestion des terminaux**.



2. Dans la zone de texte **E-mail**, saisissez le nom d'utilisateur fourni à votre utilisateur suivi du domaine de l'environnement au format `Username@domain.com` (par exemple `jdoe1@acme.com`).
3. **Saisissez l'adresse de serveur** comme suit : `<DeviceServicesURL>/DeviceServices/Discovery.aws`. N'incluez pas « https:// » dans l'URL. **Exemple** : `ds156.awmdm.com/deviceservices/discovery.aws`.
4. Sélectionnez **Continuer**.
5. Saisissez l'**ID de groupe** et sélectionnez **Suivant**.
6. Saisissez le **Nom d'utilisateur** et le **Mot de passe**, puis sélectionnez **Suivant**. Il peut s'agir de vos identifiants de services d'annuaire ou d'identifiants dédiés propres à votre environnement Workspace ONE UEM.
7. **Facultatif** : Lisez le Contrat de licence pour utilisateur final et sélectionnez **J'accepte** pour accepter les conditions d'utilisation. Cette étape est facultative et n'apparaît que si vous l'avez activée.
8. **Facultatif** : Sélectionnez **Oui** pour enregistrer vos informations de connexion.

Résultats

Le terminal tente alors de se connecter à Workspace ONE UEM. Si la connexion réussit, une icône en forme de mallette sur laquelle est inscrit Workspace ONE UEM, apparaît. Cette icône indique que vous avez réussi à vous connecter à Workspace ONE UEM.



Préenrôlement des terminaux Windows

Avec la fonction de préenrôlement des terminaux, vous pouvez configurer vos terminaux Windows pour qu'ils soient gérés par Workspace ONE UEM avant de les envoyer à vos utilisateurs finaux. Découvrez comment enrôler et configurer vos terminaux avec Workspace ONE Intelligent Hub pour le compte de vos utilisateurs finaux.

Le préenrôlement des terminaux vous permet d'enrôler votre terminal Windows dans Workspace ONE UEM. Cet enrôlement nécessite que Workspace ONE Intelligent Hub soit démarré. Une fois le terminal enrôlé, tous les profils de niveau terminal sont téléchargés sur le terminal. Une fois le terminal complètement enrôlé et configuré, vous pouvez le remettre aux utilisateurs. Lorsque l'utilisateur se connecte au terminal, Workspace ONE Intelligent Hub met à jour l'enregistrement de ce terminal dans Workspace ONE UEM console. Workspace ONE UEM réattribue le terminal à l'utilisateur et envoie au terminal tous les profils de niveau utilisateur.

Les deux méthodes de préenrôlement sont les suivantes :

- **Installation manuelle** : téléchargez et installez Workspace ONE Intelligent Hub, puis entrez les informations d'identification d'enrôlement. Pour cette méthode, les terminaux doivent être joints au domaine avant leur enrôlement.
- **Installation par ligne de commande** : téléchargez Workspace ONE Intelligent Hub, puis installez et enrôlez le terminal à l'aide de la ligne de commande.

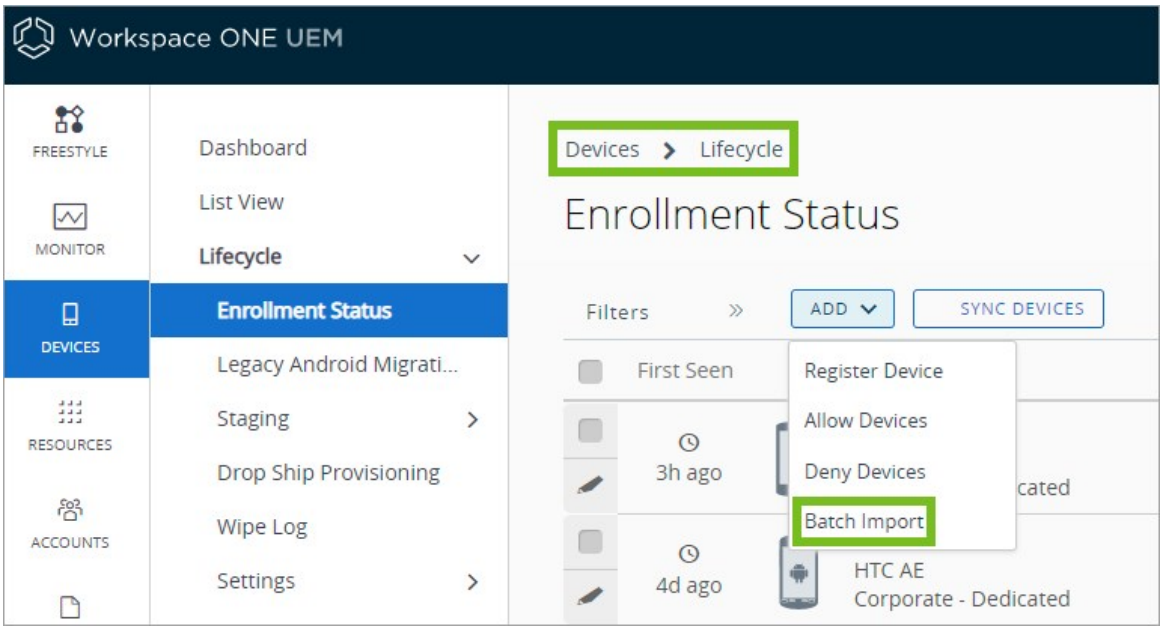
L'enrôlement se termine soit par la mise à jour du registre du terminal sur UEM Console lorsqu'un utilisateur s'enrôle dans un terminal joint au domaine, soit par la comparaison du nom d'utilisateur enrôlé à la liste des numéros de série déjà enregistrés.

Importer par lots des numéros de série de terminal

Importez les numéros de série de terminal à utiliser avec le préenrôlement des terminaux afin d'ajouter rapidement des terminaux à Workspace ONE UEM Console. L'importation par lots nécessite un fichier CSV avec tous les numéros de série à importer.

Procédure

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



2. Sélectionnez **Ajouter**, puis **Importation par lots** pour afficher l'écran **Importation par lots**.
3. Renseignez chacune des options obligatoires. **Nom du lot**, **Description du lot** et **Type de lot**.
4. 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.
5. Sélectionnez le modèle de téléchargement approprié et enregistrez le fichier de valeurs séparées par des virgules (CSV, comma-separated values) dans un emplacement accessible.
6. 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.
7. 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.
8. Cliquez sur **Enregistrer** pour terminer l'inscription pour tous les utilisateurs listés et les terminaux correspondants.

Carbon Black et Workspace ONE Intelligent Hub pour Windows

Utilisez-vous Carbon Black pour la protection des points de terminaison sur vos terminaux

Windows ? Vous pouvez installer Carbon Black sur vos terminaux Windows lorsque vous installez VMware Workspace ONE Intelligent Hub pour Windows.

Enrôlez vos terminaux Windows à l'aide du processus de préenrôlement de la ligne de commande. Entrez les paramètres d'enrôlement en mode silencieux spécifiques à Carbon Black et leurs valeurs d'URL respectives que vous avez générées dans Carbon Black. La saisie des URL générées indique à Workspace ONE Intelligent Hub qu'il doit récupérer les URL du kit de capteur Carbon Black et le fichier de configuration du capteur Carbon Black pour l'installation.

Après l'installation de Carbon Black et de VMware Workspace ONE Intelligent Hub, importez l'application publique Carbon Black dans Workspace ONE UEM Console et publiez l'application sur vos terminaux Windows.

Pour plus d'informations sur la génération des URL requises pour le kit de capteur Carbon Black et le fichier de configuration de capteur Carbon Black, accédez au contenu du *Guide de l'utilisateur Carbon Black Cloud*. Vous pouvez vous connecter à VMware Carbon Black Cloud et sélectionner **Aide** > **Guide de l'utilisateur**. Saisissez `workspace one` dans la barre de recherche et appuyez sur **Entrée**.

Où se trouvent les paramètres Carbon Black ?

Les paramètres Carbon Black sont disponibles dans cette rubrique de la section **Paramètres et valeurs de l'enrôlement silencieux**. Vous les trouverez également dans la console Carbon Black Cloud, en vous rendant dans **Inventaire > Points de terminaison > Options du capteur > Configurer un kit de capteur Workspace ONE**. Si vous ne voyez pas cette option dans la console Carbon Black Cloud, contactez votre assistance Carbon Black pour activer cette fonctionnalité.

Enrôlement par préenrôlement à l'aide de la ligne de commande

Simplifiez l'enrôlement des utilisateurs en préenrôlant les terminaux Windows Desktop à l'aide de la ligne de commande Windows. Cette méthode d'enrôlement pour Workspace ONE UEM enrôle le terminal et télécharge les profils de niveau terminal en fonction des informations d'identification d'utilisateur entrées.

Important : ne changez pas le nom du fichier AirWatchAgent.msi, car cela empêcherait la commande de préenrôlement de fonctionner. De plus, n'utilisez pas l'importation de numéros de série par lots si vous souhaitez utiliser le transfert de ligne de commande.

Remarque : N'utilisez pas ce produit pour installer Workspace ONE Intelligent Hub pour Windows en mode silencieux sur les terminaux personnels (BYOD). Si vous procédez à une installation silencieuse sur des terminaux BYOD, vous êtes seul responsable de la transmission de toutes les notifications nécessaires aux utilisateurs finaux du terminal concernant votre utilisation de l'installation silencieuse et des données collectées à partir des applications installées de cette façon. Vous êtes responsable de l'obtention des consentements légalement requis auprès des utilisateurs finaux de vos terminaux, ainsi que du respect de toutes les lois applicables.

Procédure

1. Accédez à https://getwsone.com/ pour télécharger Workspace ONE Intelligent Hub pour Windows.

   Téléchargez uniquement Workspace ONE Intelligent Hub. Ne démarrez pas l'exécutable et

ne sélectionnez pas **Exécuter**, car ces opérations démarrent un processus d'enrôlement standard, ce qui irait à l'encontre de l'objectif de l'enrôlement silencieux. Si nécessaire, déplacez Workspace ONE Intelligent Hub depuis le dossier de téléchargement vers un dossier d'un disque local ou sur le réseau.

2. Ouvrez une ligne de commande ou créez un fichier BAT, puis indiquez tous les chemins, paramètres et valeurs nécessaires.
3. Exécutez la commande.

Résultats

Après l'exécution de la commande, le terminal est enrôlé dans Workspace ONE UEM. Si le terminal est joint à un domaine, Workspace ONE Intelligent Hub met à jour le registre des terminaux dans Workspace ONE UEM console avec l'utilisateur correct.

Enrôlement par l'intermédiaire du préenrôlement manuel d'un terminal

Simplifiez l'enrôlement des utilisateurs en préenrôlant les terminaux Windows à l'aide de VMware Workspace ONE Intelligent Hub. Cette méthode d'enrôlement enrôle le terminal et télécharge les profils de niveau terminal de manière à ce que l'utilisateur n'ait qu'à se connecter au terminal pour commencer à l'utiliser.

Conditions prérequises

Ces terminaux doivent être intégrés à un domaine.

1. Rendez-vous sur https://getwsone.com/ pour télécharger le programme d'installation de VMware Workspace ONE Intelligent Hub.
2. Démarrez le programme d'installation lorsque le téléchargement est terminé.
3. Sélectionnez **Exécuter** pour commencer l'installation.
4. Sélectionnez **E-mail** si l'option Détection automatique est activée. Sinon, sélectionnez **Détails du serveur**.
5. Définissez les paramètres requis en fonction du type d'authentification sélectionné.
    1. Saisissez l'adresse e-mail pour remplir automatiquement l'écran des détails du serveur. Sélectionnez **Suivant** ; les détails sont entrés.
    2. Entrez le nom du serveur et l'ID de groupe si vous n'utilisez pas l'option Détection automatique pour définir les paramètres. Sélectionnez **Suivant**.
6. Saisissez le **Nom d'utilisateur** et le **Mot de passe** de préenrôlement, puis sélectionnez **Suivant**.
7. Remplissez les autres écrans, le cas échéant.
8. Sélectionnez **Terminer** pour terminer l'enrôlement.

Résultats

Dès que Workspace ONE Intelligent Hub détecte un utilisateur de préenrôlement, l'écouteur de Workspace ONE Intelligent Hub s'exécute et écoute à la prochaine connexion Windows. Lorsque l'utilisateur se connecte au terminal, l'écouteur de Workspace ONE Intelligent Hub lit l'UPN et l'adresse e-mail de l'utilisateur à partir du registre du terminal. Ces informations sont envoyées à

Workspace ONE UEM console et le registre du terminal est mis à jour afin d'enregistrer le terminal pour l'utilisateur.

Paramètres et valeurs de l'enrôlement silencieux

L'enrôlement silencieux requiert des saisies sur la ligne de commande ou un fichier BAT afin de contrôler la façon dont VMware Workspace ONE Intelligent Hub se télécharge et s'installe sur les terminaux Windows.

Remarque : N'utilisez pas ce produit pour installer Workspace ONE Intelligent Hub pour Windows en mode silencieux sur les terminaux personnels (BYOD). Si vous procédez à une installation silencieuse sur des terminaux BYOD, vous êtes seul responsable de la transmission de toutes les notifications nécessaires aux utilisateurs finaux du terminal concernant votre utilisation de l'installation silencieuse et des données collectées à partir des applications installées de cette façon. Vous êtes responsable de l'obtention des consentements légalement requis auprès des utilisateurs finaux de vos terminaux, ainsi que du respect de toutes les lois applicables.

Les tableaux suivants répertorient tous les paramètres d'enrôlement que vous pouvez saisir sur une ligne de commande ou dans un fichier BAT ainsi que les valeurs respectives pour chaque paramètre. Si vous effectuez l'enrôlement pour le compte d'autres personnes, assurez-vous d'utiliser les paramètres Enrôlement pour le compte d'un utilisateur.

Paramètres généraux

Paramètres d'enrôlement	Valeur à ajouter au paramètre
Tous les paramètres MSI	Ces paramètres contrôlent le comportement d'installation des applications. `/quiet` - Complètement silencieux `/q` - Contrôle les niveaux d'interface utilisateur pour l'installation `passive` - Contrôle minimal de l'utilisateur lui permettant de guider l'application `/L` - Niveaux et chemins d'accès de journalisation. Pour plus d'informations, reportez-vous à https://docs.microsoft.com/fr-fr/windows/win32/msi/command-line-options.
ASSIGNTOLOGGEDINUSER	Sélectionnez `Y` pour attribuer le terminal à l'utilisateur de domaine connecté. Entrez ce paramètre comme dernier argument dans la ligne de commande.
DEVICEOWNERSHIPTYPE ^	Sélectionnez `CD` pour Entreprise dédiée. Sélectionnez `CS` pour Entreprise partagée. Sélectionnez `EO` pour Employé propriétaire. Sélectionnez `N` pour Aucun.
DOWNLOADSBUNDLE	Ce paramètre contrôle le téléchargement de l'application Workspace ONE lors de l'enrôlement. Sélectionnez `TRUE` pour télécharger le programme d'installation de l'application Workspace ONE lors de l'installation de Workspace ONE Intelligent Hub. Si vous enrôlez un terminal à l'aide de Workspace ONE Intelligent Hub, l'installation de Workspace ONE n'est pas facultative. Si vous ne définissez pas DOWNLOADSBUNDLE sur `TRUE`, le programme d'installation de Workspace ONE ne se télécharge pas, quel que soit le niveau d'interface utilisateur utilisé.
ENROLL	Sélectionnez `Y` pour effectuer un enrôlement. Sélectionnez `N` pour choisir l'image uniquement. L'agent tentera l'enrôlement en mode silencieux uniquement si ce paramètre est défini sur `Y`.

Paramètres d'enrôlement	Valeur à ajouter au paramètre
IMAGE	Cet indicateur est prioritaire sur tout. S'il est défini sur `Y`, l'agent est placé en mode image. Sélectionnez `Y` pour choisir l'image. Sélectionnez `N` pour l'enrôlement.
INSTALLDIR^	Saisissez le chemin d'accès au répertoire si vous souhaitez changer le chemin d'installation. **Remarque** : Si ce paramètre n'est pas présent, Workspace ONE Intelligent Hub utilise le chemin par défaut : `C:\Program Files (x86)\AirWatch`.
LGName	Saisissez le nom du groupe organisationnel.
PASSWORD	Saisissez le mot de passe de l'utilisateur que vous enrôlez ou le mot de passe d'utilisateur de préenrôlement en cas de préenrôlement du terminal pour le compte d'un utilisateur.
SERVER	Saisissez l'URL d'enrôlement.
USERNAME	Saisissez le nom d'utilisateur de l'utilisateur que vous enrôlez ou le nom d'utilisateur de préenrôlement en cas de préenrôlement du terminal pour le compte d'un utilisateur.

Les éléments signalés par un accent circonflexe (^) sont facultatifs.

Paramètres Enrôlement pour le compte d'un utilisateur

Paramètres d'enrôlement	Valeur à ajouter au paramètre
SECURITYTYPE	Workflow EOBO uniquement : Utilisez ce paramètre si le compte utilisateur est ajouté à Workspace ONE UEM console durant le processus d'enrôlement. Sélectionnez `D` pour l'**annuaire**. Sélectionnez `B` pour l'**utilisateur de base**.
STAGEEMAIL^	Workflow EOBO uniquement : Saisissez l'adresse de messagerie pour l'utilisateur que vous enrôlez.
STAGEEMAILUSRNAME^	Workflow EOBO uniquement : Saisissez le nom d'utilisateur de messagerie pour l'utilisateur que vous enrôlez.
STAGEPASSWORD	Workflow EOBO uniquement : Saisissez le mot de passe de messagerie pour l'utilisateur que vous enrôlez.
STAGEUSERNAME	Workflow EOBO uniquement : Saisissez le nom d'utilisateur pour l'utilisateur d'enrôlement.

Les éléments signalés par un accent circonflexe (^) sont facultatifs.

Paramètres Carbon Black

Paramètres d'enrôlement	Valeur à ajouter au paramètre

CBSENSORCONFIGURL^	Utilisez ce paramètre pour demander à Workspace ONE Intelligent Hub pour Windows de récupérer l'URL du fichier de configuration Carbon Black. Entrez l'URL du fichier de configuration du capteur que vous avez générée dans Carbon Black.
CBSENSORURL^	Utilisez ce paramètre pour demander à Workspace ONE Intelligent Hub pour Windows de récupérer l'URL du kit de capteur Carbon Black applicable. Entrez l'URL du kit de capteur que vous avez générée dans Carbon Black.

Les éléments signalés par un accent circonflexe (^) sont facultatifs.

Exemples d'enrôlement silencieux

Découvrez des exemples de cas d'utilisation différents qui utilisent des paramètres d'enrôlement et les valeurs que vous pouvez saisir sur une ligne de commande ou utiliser afin de créer un fichier BAT. L'exécution de n'importe lequel de ces exemples enrôle le terminal de façon silencieuse sans que l'utilisateur ait à cliquer sur les boutons de confirmation.

- **Installation de l'agent pour l'image seulement sans enrôlement**

  Voici un exemple d'installation de Workspace ONE Intelligent Hub pour l'image seulement, sans enrôlement, à l'aide des paramètres requis pour ce type d'installation.

  ```
  AirwatchAgent.msi /quiet ENROLL=N IMAGE=Y
  ```

- **Enrôlement utilisateur de base**

  Voici un exemple d'utilisation des paramètres minimaux requis pour l'enrôlement de base uniquement :

  ```
  AirwatchAgent.msi /quiet ENROLL=YIMAGE=n SERVER=companyURL.com LGName=locationg
  roupid USERNAME=TestUsr PASSWORD=test
  ```

- **Workspace ONE Intelligent Hub installé ailleurs**

  Voici un exemple de fichier AirwatchAgent.msi situé dans un emplacement différent :

  ```
  C:AirwatchAgent.msi /quiet ENROLL=Y IMAGE=n SERVER=companyURL.com LGName=locati
  ongroupid USERNAME=TestUsr PASSWORD=test
  ```

- **Répertoire d'installation et Workspace ONE Intelligent Hub sur lecteur réseau**

  Voici un exemple d'utilisation du paramètre pour le répertoire d'installation avec Workspace ONE Intelligent Hub sur un lecteur réseau.

  Important : ajoutez des guillemets supplémentaires pour le paramètre INSTALLDIR en cas d'espace dans celui-ci.

  ```
  Q:AirwatchAgent.msi /quiet INSTALLDIR="E:Install Win32" ENROLL=Y IMAGE=n SERVER
  =companyURL.com LGName=locationgroupid USERNAME=TestUsr PASSWORD=test
  ```

- **Paramètres et valeurs disponibles**

  L'extrait suivant est un exemple de syntaxe utilisant la plupart des paramètres et valeurs disponibles.

```
msiexec.exe /I "<Path>AirwatchAgent.msi" /quiet ENROLL=<Y/N>IMAGE=<Y/N>SERVER=<
CompanyURL>LGNAME=<Location Group ID>USERNAME=<Staging Username>PASSWORD=<Stagi
ng Username Password>STAGEUSERNAME=<Enrolling Username>SECURITYTYPE=<D/B>STAGEE
MAILUSRNAME=<User Enrolling>STAGEPASSWORD=<Password for User Enrolling>STAGEEMA
IL=<Email Address for User Enrolling>DEVICEOWNERSHIPTYPE<CD/CS/EO/N>ASSIGNTOLOG
GEDINUSER=<Y/N>
```

Intégration de Workspace ONE UEM et Azure AD

Grâce à l'intégration avec Microsoft Azure Active Directory, vous pouvez enrôler automatiquement vos terminaux Windows dans Workspace ONE UEM avec une interaction minimale de l'utilisateur final. Découvrez comment l'intégration d'Azure AD simplifie l'enrôlement de vos terminaux Windows.

Pour pouvoir enrôler vos terminaux à l'aide de l'intégration d'Azure AD, vous devez configurer Workspace ONE UEM et Azure AD. La configuration nécessite la saisie d'informations dans vos déploiements Azure AD et Workspace ONE UEM pour faciliter la communication. L'installation est différente en fonction de votre environnement. Suivez la procédure appropriée pour votre déploiement SaaS ou sur site.

L'enrôlement de l'intégration Azure AD prend en charge trois flux d'enrôlement différents.

- Rejoindre Azure AD
- Enrôlement immédiat
- Enrôlement Office 365

Toutes les méthodes nécessitent la configuration de l'intégration d'Azure AD à Workspace ONE UEM.

Important : L'enrôlement via l'intégration d'Azure AD requiert Windows et une licence Azure Active Directory Premium.

Environnements SaaS : Azure AD en tant que service d'identité

Avant d'utiliser Azure AD pour enrôler vos terminaux Windows, vous devez configurer Workspace ONE UEM pour qu'il utilise Azure AD en tant que service d'identité. L'activation d'Azure AD nécessite l'entrée des données dans le portail de gestion Azure et dans Workspace ONE UEM. Utilisez les onglets de votre navigateur pour ouvrir les deux instances afin d'entrer plus facilement les données dans les deux consoles.

Conditions prérequises

- Vous devez posséder un abonnement Premium Azure AD P1 ou P2 pour intégrer Azure AD à Workspace ONE UEM.
- L'intégration d'Azure AD à Workspace ONE UEM doit être configurée au niveau du tenant où le service Active Directory (tel que LDAP) est configuré. -Si vous avez associé un nom de domaine personnalisé à votre instance SaaS, reportez-vous à la section suivante (environnements sur site ou environnements SaaS avec un nom de domaine personnalisé) pour obtenir ces instructions spécifiques.

Important : Commencer par configurer et enregistrer LDAP
Si vous définissez **Paramètre actuel** sur **Remplacer** sur la page des paramètres système des services

d'annuaire dans Workspace ONE UEM, vous devez configurer et enregistrer les paramètres LDAP avant d'activer Azure AD pour les services d'identité.

Procédure

1. Dans Workspace ONE UEM, activez l'intégration à Azure AD, entrez l'ID de locataire Azure AD et récupérez les URL d'enrôlement MDM pour les entrer dans Azure.
    1. Sélectionnez le groupe organisationnel approprié.
    2. Naviguez vers **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > Services d'annuaire**.
    3. Dans l'onglet **Serveur**, activez **Intégration Azure AD**.
    4. Dans un autre onglet de votre navigateur, connectez-vous au portail de gestion Azure avec votre compte Microsoft ou votre compte d'organisation pour obtenir l'**ID de locataire Azure AD**.
        1. Sélectionnez **Azure Active Directory** pour afficher la page **Présentation**.
        2. Copiez l'**ID de locataire Azure AD** sur la page **Présentation** d'Azure AD.
    5. Revenez à l'instance de Workspace ONE UEM Console et collez l'ID de locataire Azure AD dans la zone de texte **ID d'annuaire**.
    6. Dans l'instance de Workspace ONE UEM, activez **Utiliser Azure AD pour les services d'identité**.
       Notez l'**URL de détection MDM** et l'**URL des conditions d'utilisation MDM**, car vous devez les entrer dans Azure. Vous pouvez les copier entre onglets si vous utilisez plusieurs onglets de navigateur ou vous pouvez les copier quelque part sur votre PC.
2. Dans Azure AD, ajoutez l'application Workspace ONE UEM et les URL MDM.
    1. Dans l'instance du portail de gestion Azure, sélectionnez votre annuaire et accédez à l'onglet **Mobilité (MDM et MAM)**.
    2. Sélectionnez **Ajouter une application**, sélectionnez l'application **AirWatch by VMware**, puis choisissez **Ajouter**.
    3. Sélectionnez l'application **AirWatch by VMware** que vous venez d'ajouter pour modifier la valeur du champ Portée de l'utilisateur GDR en **Tout**.
    4. Copiez votre **URL des conditions d'utilisation MDM** à partir de votre PC ou de l'onglet du navigateur disposant de l'instance de Workspace ONE UEM, puis collez-la dans la zone de texte **URL des conditions d'utilisation MDM** dans Azure.
    5. Copiez votre **URL de détection MDM** à partir de votre PC ou de l'onglet du navigateur disposant de l'instance de Workspace ONE UEM Console puis collez-la dans la zone de texte **URL de détection MDM** dans Azure.
    6. Enregistrez vos paramètres.
3. Dans Workspace ONE UEM, entrez le domaine Azure AD **Principal** et enregistrez les paramètres.
    1. Dans l'instance du portail de gestion Azure, accédez à la page **Aperçu** d'Azure AD et copiez le domaine **Principal** à partir de la page **Aperçu** d'Azure AD.
    2. Sur l'onglet du navigateur avec l'instance de Workspace ONE UEM Console, collez la chaîne du domaine **Principal** dans la zone de texte **Nom du locataire**.

3. Enregistrez les paramètres sur la page **Services d'annuaire** de Workspace ONE UEM.

4. Dans Azure, attribuez des licences Premium.
    1. Dans la console Microsoft Azure, sélectionnez **Azure Active Directory > Licences**.
    2. Sélectionnez **Tous les produits** et sélectionnez la licence appropriée dans la liste.
    3. Sélectionnez **Attribuer**, sélectionnez les utilisateurs ou les groupes pour la licence, puis sélectionnez sur **Attribuer** pour terminer la procédure.

Environnements sur site ou environnement SaaS avec un nom de domaine personnalisé : Azure AD en tant que service d'identité

Avant d'utiliser Azure AD pour enrôler vos terminaux Windows, vous devez configurer Workspace ONE UEM pour qu'il utilise Azure AD en tant que service d'identité. L'activation d'Azure AD nécessite l'entrée des données dans le portail de gestion Azure et dans Workspace ONE UEM. Utilisez les onglets de votre navigateur pour ouvrir les deux instances afin d'entrer plus facilement les données dans les deux consoles.

Conditions prérequises

- Vous devez posséder un abonnement Premium Azure AD P1 ou P2 pour intégrer Azure AD à Workspace ONE UEM.
- L'intégration d'Azure AD à Workspace ONE UEM doit être configurée au niveau du tenant où le service Active Directory (tel que LDAP) est configuré.
- Dans le portail Active Directory Azure, ajoutez un domaine personnalisé pour votre nom de domaine avec Microsoft Azure. Suivez la documentation de Microsoft à l'adresse Ajouter votre nom de domaine personnalisé à l'aide du portail Active Directory Azure.

Important : Commencer par configurer et enregistrer LDAP
Si vous définissez **Paramètre actuel** sur **Remplacer** sur la page des paramètres système des **Services d'annuaire** dans Workspace ONE UEM, vous devez configurer et enregistrer les paramètres LDAP avant d'activer Azure AD pour les services d'identité.

Procédure

1. Dans Workspace ONE UEM, activez l'intégration à Azure AD, entrez l'ID de locataire Azure AD et récupérez les URL d'enrôlement MDM pour les entrer dans Azure.
    1. Sélectionnez le groupe organisationnel approprié.
    2. Naviguez vers **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > Services d'annuaire**.
    3. Dans l'onglet **Serveur**, activez **Intégration Azure AD**.
    4. Dans un autre onglet de votre navigateur, connectez-vous au portail de gestion Azure avec votre compte Microsoft ou votre compte organisationnel et obtenez l'**ID de locataire Azure AD**.
        1. Sélectionnez **Azure Active Directory** pour afficher la page **Présentation**.
        2. Copiez l'**ID de locataire Azure AD** sur la page **Aperçu** d'Azure AD.
    5. Accédez à l'instance de Workspace ONE UEM Console et collez l'ID de locataire

Azure AD dans la zone de texte **ID d'annuaire**.

6. Dans l'instance de Workspace ONE UEM, activez **Utiliser Azure AD pour les services d'identité**.
   Notez l'**URL de détection MDM** et l'**URL des conditions d'utilisation MDM**, car vous devez les entrer dans Azure. Vous pouvez les copier entre onglets si vous utilisez plusieurs onglets de navigateur ou vous pouvez les copier quelque part sur votre PC.

2. Dans Azure AD, ajoutez la version sur site de l'application Workspace ONE UEM et ajoutez les URL MDM.
   1. Dans l'instance du portail de gestion Azure, sélectionnez votre annuaire et accédez à l'onglet **Mobilité (MDM et MAM)**.
   2. Sélectionnez **Ajouter une application** et choisissez l'application **MDM sur site**. Choisissez ensuite **Ajouter**.
   3. Sélectionnez l'application **MDM sur site** que vous venez d'ajouter pour définir la **Portée de l'utilisateur MDM** sur **Tout** ou **Certains**.
   4. Sélectionnez un groupe d'utilisateurs.
   5. Copiez votre **URL des conditions d'utilisation MDM** à partir de votre PC ou de l'onglet du navigateur disposant de l'instance de Workspace ONE UEM, puis collez-la dans la zone de texte **URL des conditions d'utilisation MDM** dans Azure.
   6. Copiez votre **URL de détection MDM** à partir de votre PC ou de l'onglet du navigateur disposant de l'instance de Workspace ONE UEM Console puis collez-la dans la zone de texte **URL de détection MDM** dans Azure.
   7. Enregistrez vos paramètres.
3. Dans le portail de gestion Azure, ajoutez l'URL des services de terminal Workspace ONE UEM.
   1. Dans l'instance Workspace ONE UEM, accédez à **Groupes et paramètres > Tous les paramètres > Système > Avancés > URL de sites** et copiez l'**URL des services de terminal**.
   2. Dans l'instance du portail de gestion Azure, sélectionnez **Paramètres d'application MDM sur site > Exposer une API**.
   3. Sélectionnez **Modifier** pour **URI d'ID d'application** et entrez l'URL des services de votre terminal dans la zone de texte **URI d'ID d'application**.
   4. Enregistrez les paramètres.
      Remarque : L'enregistrement des paramètres fonctionne si vous avez effectué la tâche préalable d'ajout d'un nom de domaine personnalisé. Si vous voyez une erreur, vérifiez que vous avez ajouté votre domaine personnalisé à Azure.
4. Dans Workspace ONE UEM, entrez le domaine Azure AD **Principal** et enregistrez les paramètres.
   1. Dans l'instance du portail de gestion Azure, accédez à la page **Aperçu** d'Azure AD et copiez le domaine **Principal** à partir de la page **Aperçu** d'Azure AD.
   2. Dans l'instance de Workspace ONE UEM Console, collez la chaîne de domaine **Principal** dans la zone de texte **Nom du locataire**.

3. Enregistrez les paramètres sur la page **Services d'annuaire** de Workspace ONE UEM.

5. Dans Azure, attribuez des licences Premium.
    1. Dans la console Microsoft Azure, sélectionnez **Azure Active Directory > Licences**.
    2. Sélectionnez **Tous les produits** et sélectionnez la licence appropriée dans la liste.
    3. Sélectionnez **Attribuer**, sélectionnez les utilisateurs ou les groupes pour la licence, puis sélectionnez sur **Attribuer** pour terminer la procédure.

Enrôler un terminal avec Azure AD

Enrôlez des terminaux avec l'intégration d'Azure AD pour enrôler automatiquement un terminal dans le groupe organisationnel approprié de Workspace ONE UEM. Les terminaux enrôlés par l'intermédiaire d'Azure AD sont complètement joints, ce qui signifie que tous les utilisateurs de ces terminaux joignent le domaine.

Ce flux d'enrôlement s'adresse aux terminaux qui n'ont pas encore joint Azure AD.

Procédure

1. Sur le terminal Windows, accédez à **Paramètres > Comptes > Accès professionnel ou scolaire**. Sélectionnez **Continuer**.
2. Saisissez votre **adresse e-mail**. Sélectionnez **Suivant**.
3. Assurez-vous que la page d'accueil de Workspace ONE UEM s'affiche. Sélectionnez **Continuer**.
4. Sélectionnez **J'accepte** si les termes du contrat sont activés.
5. Sélectionnez **Joindre** pour confirmer l'enrôlement à Workspace ONE UEM.
6. Sélectionnez **Terminer** pour finaliser l'enrôlement de votre terminal à Workspace ONE UEM. Votre terminal télécharge à présent les politiques et profils applicables.

Enrôler un terminal Azure AD géré dans Workspace ONE UEM

Les terminaux joints à Azure AD utilisent un flux d'enrôlement différent de ceux enrôlés par le biais d'une intégration avec Azure AD. Utilisez ce flux d'enrôlement pour enrôler un terminal déjà joint à Azure AD dans Workspace ONE UEM.

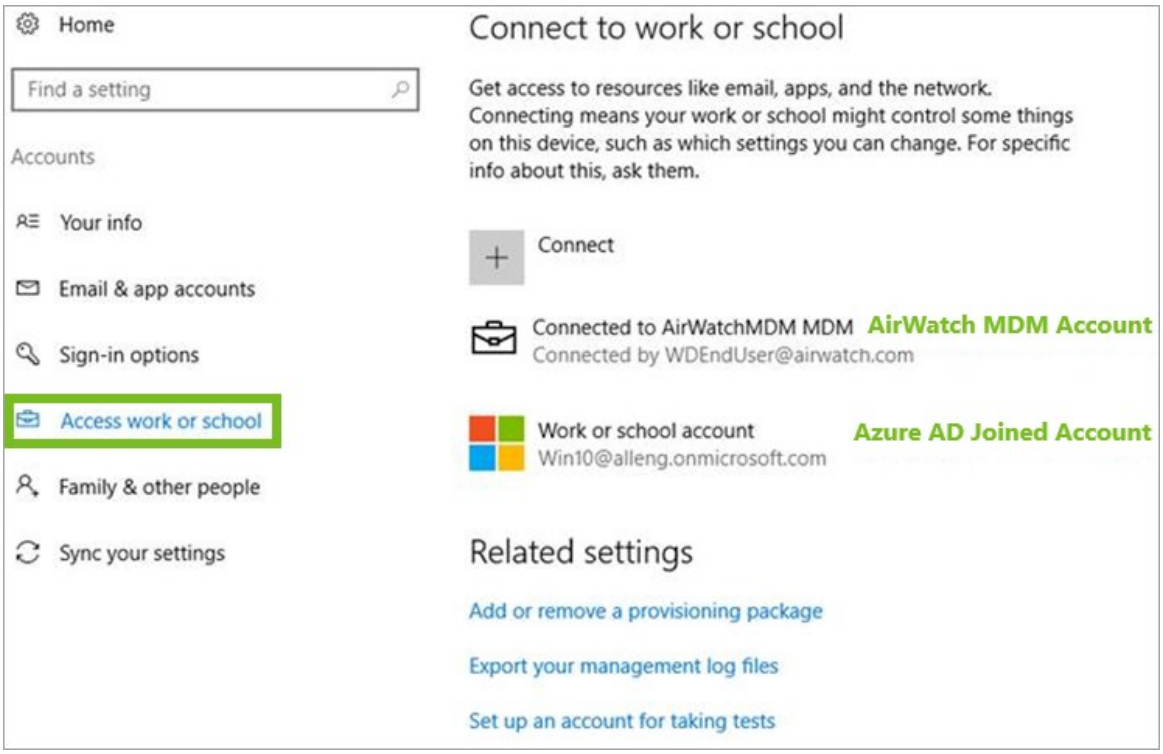
Conditions prérequises

- Système d'exploitation Windows – build 14393.82 et versions supérieures.
- Mise à jour KB3176934 installée.
- Aucune application MDM installée sous votre portail de gestion Azure AD.
- Compte Azure AD configuré sur le terminal

Procédure

1. Sur le terminal, naviguez vers **Paramètres > Comptes > Accès professionnel ou scolaire** et sélectionnez **Enrôler uniquement sur le gestionnaire de périphériques mobiles**. Vous pouvez également enrôler par l'intermédiaire de Workspace ONE Intelligent Hub pour Windows.

2. Terminez le processus d'enrôlement. Vous devez saisir une adresse e-mail avec un domaine différent de celui de votre compte Azure AD.
    1. Si vous utilisez la détection automatique pour Windows, consultez la section Enrôlement par l'intermédiaire de Work Access avec la détection automatique pour Windows.
    2. Si vous n'utilisez pas la détection automatique pour Windows, consultez la section Enrôlement par l'intermédiaire de Work Access sans la détection automatique pour Windows.
3. Accédez à **Paramètres > Comptes > Accès** professionnel ou scolaire et assurez-vous qu'un compte Azure AD et un compte Workspace ONE UEM MDM ont bien été ajoutés.



Enrôlement en mode OOBE (Out-of-Box Experience)

L'enrôlement en mode OOBE (Out-of-Box Experience) permet d'enrôler automatiquement un terminal dans le groupe organisationnel approprié au cours de la configuration initiale d'un terminal Windows.

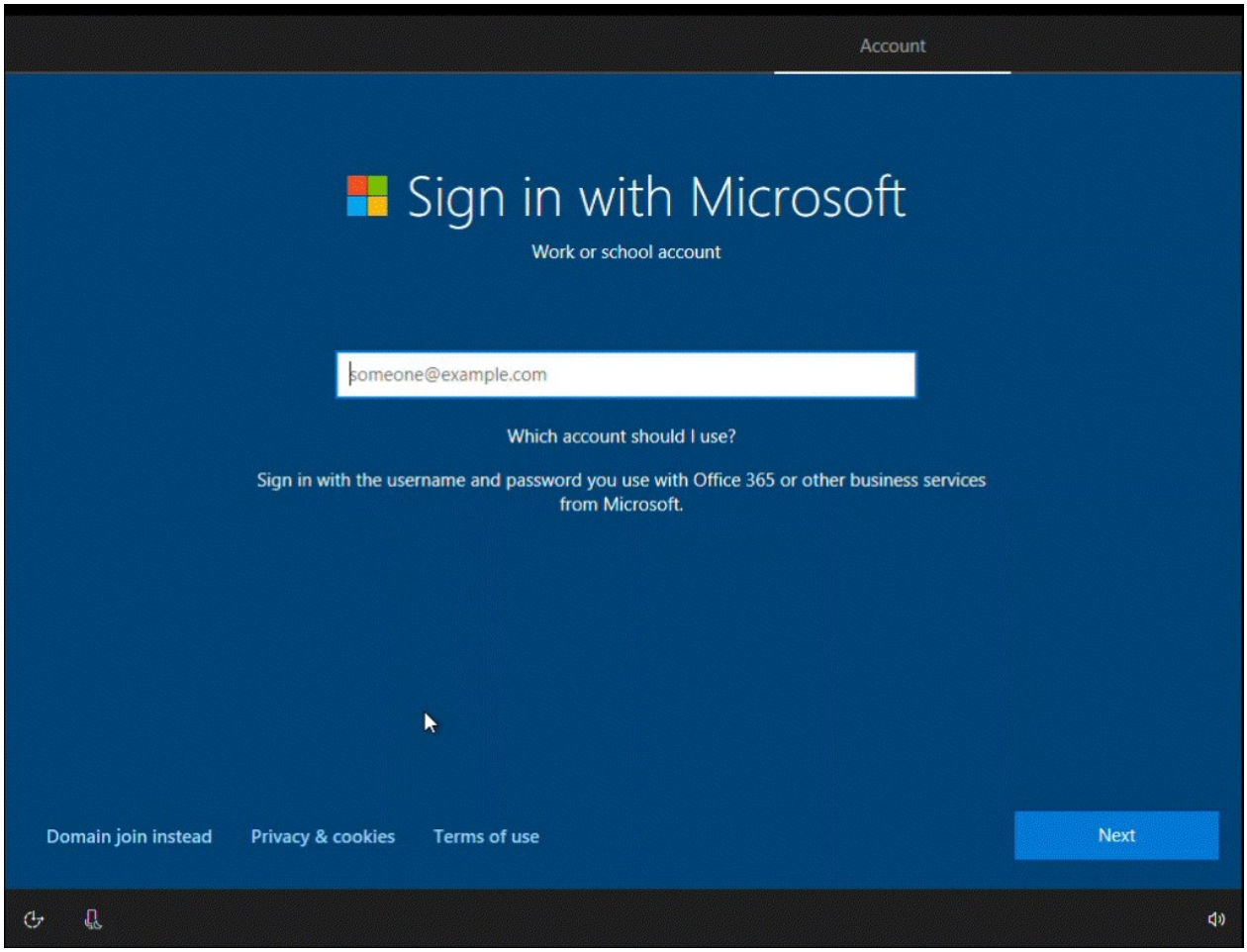
Important : Le flux d'enrôlement OOBE ne prend pas en charge l'effacement des données professionnelles. Si vous effectuez un effacement des données professionnelles, les utilisateurs ne peuvent pas se connecter au terminal, car la connexion à Azure AD a été interrompue. Vous devez créer un compte d'administrateur local avant d'envoyer un effacement des données professionnelles, faute de quoi vous êtes déconnecté de force du terminal et obligé de réinitialiser celui-ci.

Remarque : Les profils des paramètres personnalisés ne peuvent pas être suivis lors de l'OOBE et ne s'appliqueront pas lors du provisionnement.

Conditions prérequises

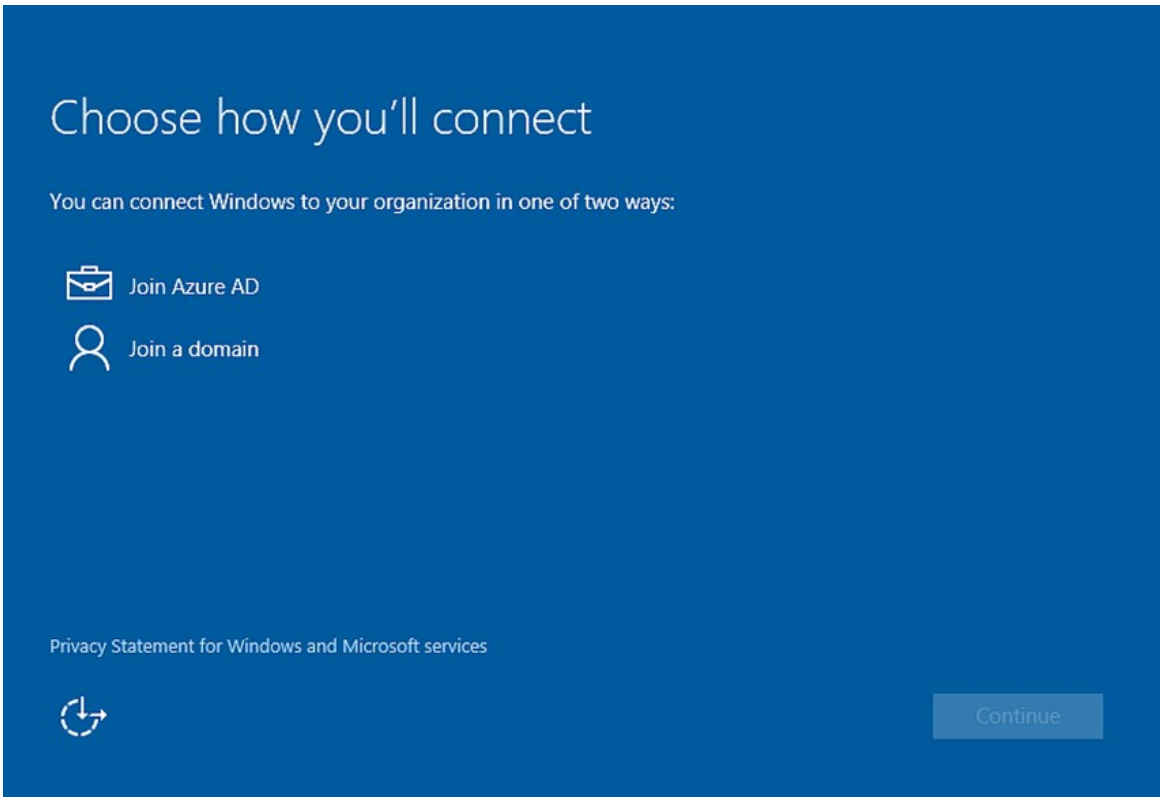
Le processus OOBE peut prendre un certain temps sur les terminaux des utilisateurs finaux. Envisagez d'activer l'affichage de la progression pour le statut de l'installation. Cet affichage permet

aux utilisateurs finaux de savoir où ils en sont dans le processus. Pour activer l'affichage, accédez à **Groupes et paramètres** > **Tous les paramètres** > **Général** > **Enrôlement** > **Invite facultative**. Pour afficher l'état des profils lors de l'enrôlement, vous devez activer l'option **Suivre l'état du profil lors du provisionnement OOBE** dans les paramètres du profil dans l'onglet **Général**.

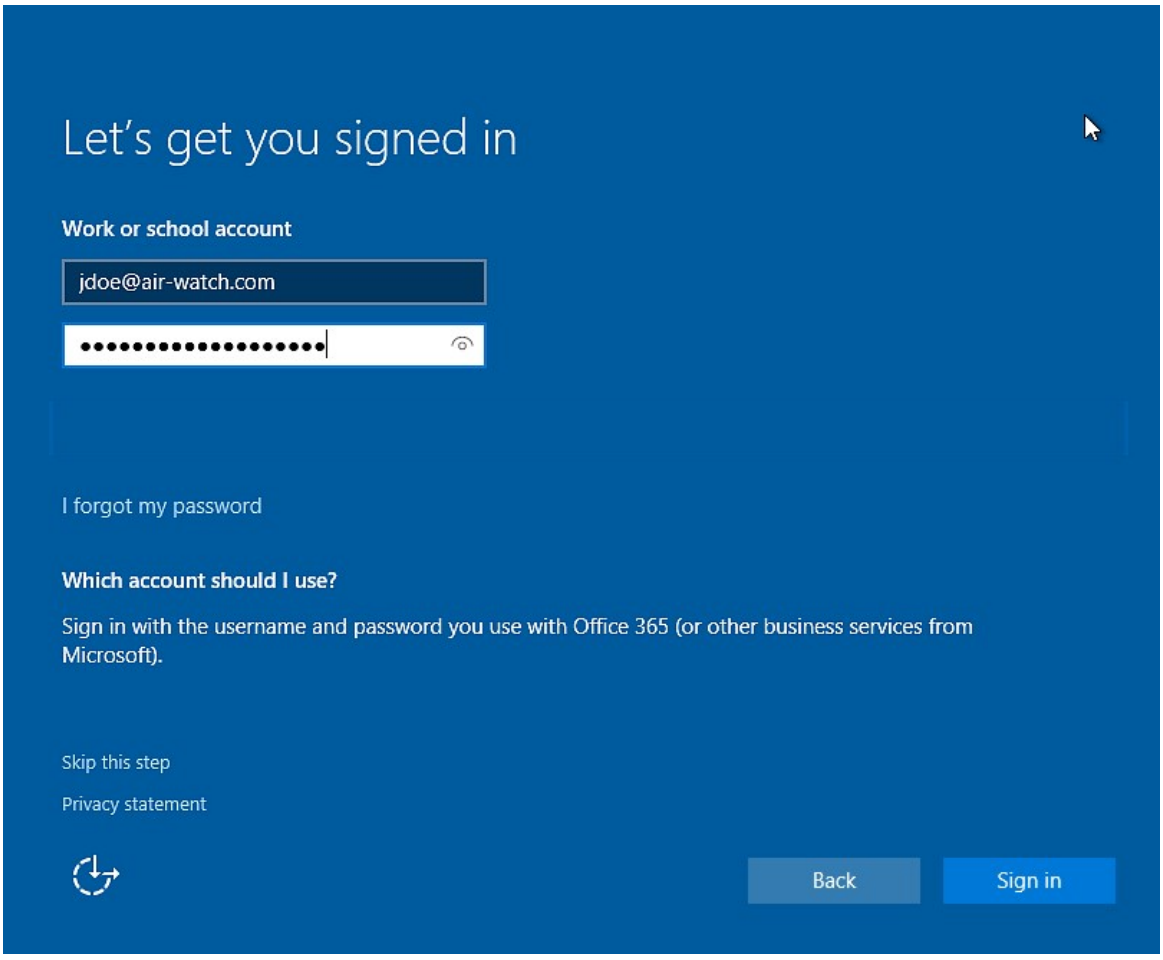


Procédure

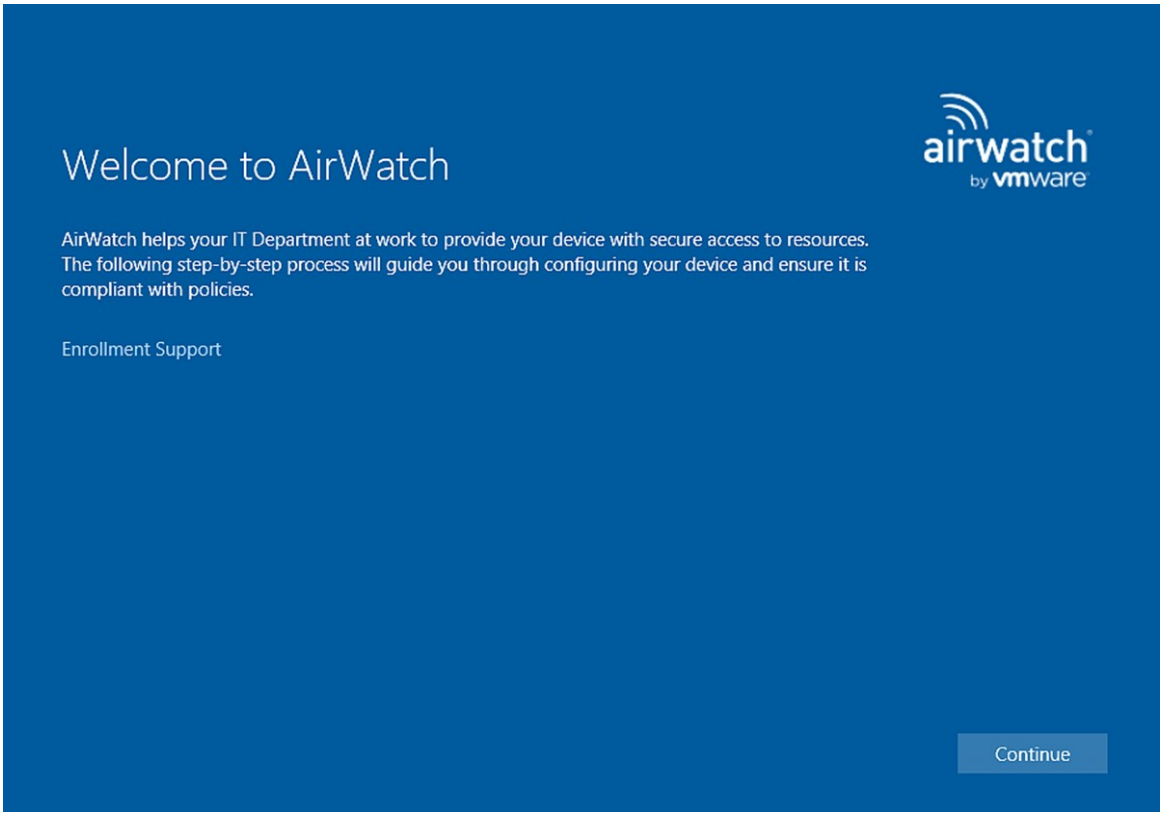
1. Mettez le terminal sous tension et suivez les étapes ci-dessous jusqu'à atteindre l'écran **Choisissez votre mode de connexion**.



2. Sélectionnez **Joindre Azure AD**. Sélectionnez **Continuer**.
3. Saisissez votre adresse e-mail Azure AD/Workspace ONE UEM en tant que **Compte professionnel ou scolaire**.



4. Saisissez votre **Mot de passe**. Sélectionnez **Se connecter**.
5. Assurez-vous que l'écran **Bienvenue dans AirWatch** apparaît. Sélectionnez **Continuer**.



6. Sélectionnez le type de **Propriété du terminal** et saisissez le **Numéro d'actif**, le cas échéant. Sélectionnez **Suivant**.
7. Sélectionnez **J'accepte** si les termes du contrat sont activés.
8. Sélectionnez **Joindre** pour confirmer l'enrôlement à Workspace ONE UEM.
9. Sélectionnez **Terminer** pour finaliser l'enrôlement de votre terminal à Workspace ONE UEM. Votre terminal télécharge à présent les politiques et profils applicables.

Enrôlement via les applications Office 365

Si votre organisation utilise Office 365 et l'intégration Azure AD, les utilisateurs peuvent enrôler leurs terminaux lorsqu'ils ouvrent une application Office 365 pour la première fois.

Procédure

1. Sélectionnez **Ajouter un compte professionnel** lorsque vous ouvrez une application Office 365 pour la première fois.
2. Saisissez votre **Adresse e-mail** et votre **Mot de passe**. Sélectionnez **Se connecter**.
3. Assurez-vous que la page d'accueil de Workspace ONE UEM s'affiche. Sélectionnez **Continuer**.
4. Sélectionnez **J'accepte** si les termes du contrat sont activés.
5. Sélectionnez **Joindre** pour confirmer l'enrôlement à Workspace ONE UEM.
6. Sélectionnez **Terminer** pour finaliser l'enrôlement de votre terminal à Workspace ONE UEM.

Votre terminal télécharge à présent les politiques et profils applicables.

Provisionnement et enrôlement par lots pour les terminaux Windows

Le provisionnement par lots vous permet de créer un package préconfiguré qui préenrôle les terminaux Windows, puis les enrôle dans Workspace ONE UEM. Apprenez à utiliser le provisionnement par lots pour enrôler et configurer plusieurs terminaux avec un compte utilisateur standard.

Ce flux d'enrôlement est la seule méthode permettant d'enrôler un terminal avec un compte utilisateur standard. Les autorisations d'administration sont encore nécessaires pour exécuter le package préconfiguré. Le provisionnement par lots prend uniquement en charge le préenrôlement standard d'un utilisateur unique.

Pour utiliser le provisionnement par lots, téléchargez le kit Microsoft Assessment and Development Kit et installez l'outil ICD (Imaging and Configuration Designer). L'outil ICD crée des packages de provisionnement utilisés pour créer des images des terminaux. Dans le cadre de ces packages de provisionnement, vous pouvez utiliser des paramètres de configuration Workspace ONE UEM de manière à ce que les terminaux provisionnés soient enrôlés automatiquement dans Workspace ONE UEM lors de la première utilisation immédiate (mode OOBE).

Pour mapper automatiquement les terminaux vers l'utilisateur approprié, enregistrez les terminaux par utilisateur ou à l'aide d'une importation par lots avant de créer le package de provisionnement.

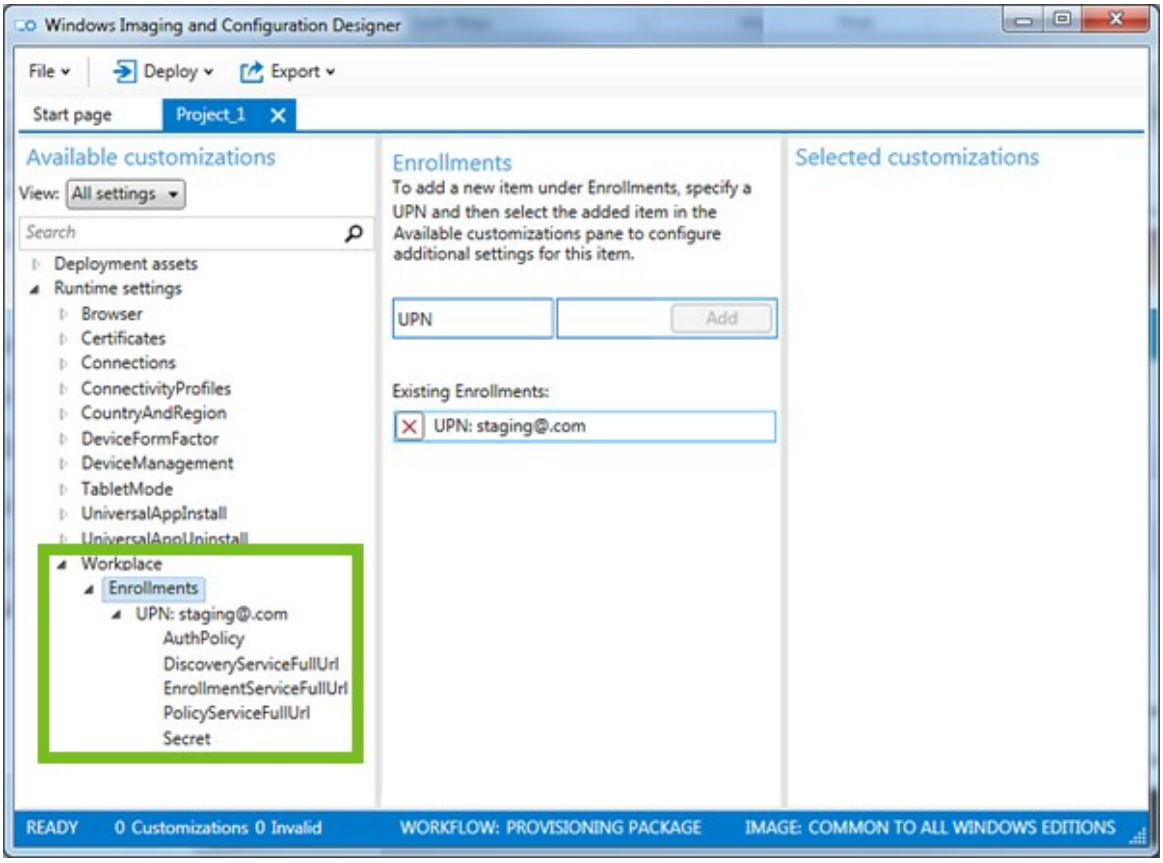
Enrôlement avec le provisionnement par lots

L'outil Microsoft Imaging and Configuration Designer vous permet de créer rapidement et facilement un package de provisionnement pour enrôler plusieurs terminaux Windows dans Workspace ONE UEM. Une fois le package installé, le terminal s'enrôle automatiquement dans Workspace ONE UEM.

Procédure

1. Téléchargez le kit Microsoft Assessment and Deployment Kit pour Windows et installez l'outil ICD (Imaging and Configuration Designer) de Windows.
2. Démarrez l'outil ICD Windows et sélectionnez **Nouveau package de provisionnement**.
3. Entrez un **nom de projet** et sélectionnez les paramètres d'affichage et de configuration. Le choix type est l'option **Commun à toutes les éditions de Windows Desktop**.
4. (Facultatif) Importez un package de provisionnement pour créer un package de provisionnement basé sur les paramètres d'un package précédent.
5. Naviguez vers **Paramètres d'exécution > Espace de travail > Enrôlements**.
6. Dans Workspace ONE UEM console, accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Windows > Windows Desktop > Préenrôlement et provisionnement**. Lorsque vous accédez à cette page de paramètres, un utilisateur de préenrôlement est créé et les URL relatives à l'utilisateur de préenrôlement créé s'affichent. Vous pouvez créer votre propre utilisateur de préenrôlement pour le provisionnement par lots, mais les paramètres de cette page ne s'appliquent à aucun utilisateur créé.
7. Copiez l'**UPN** et collez-le dans la zone de texte **UPN** de l'outil ICD.

8. Sélectionnez la flèche vers le bas en regard de l'option **Enrôlements** dans la fenêtre **Personnalisations disponibles**.



9. Configurez les paramètres suivants.
    1. Sélectionnez **AuthPolicy**, puis sélectionnez la valeur affichée dans Workspace ONE UEM console.
    2. Sélectionnez **DiscoveryServiceFullURL**, puis copiez l'URL affichée dans Workspace ONE UEM console.
    3. Sélectionnez **EnrollmentServiceFullURL**, puis copiez l'URL affichée dans Workspace ONE UEM console.
    4. Sélectionnez **PolicyServiceFullURL**, puis copiez l'URL affichée dans Workspace ONE UEM console.
    5. Sélectionnez **Secret**, puis copiez la valeur affichée dans Workspace ONE UEM console.
10. Sélectionnez **Fichier > Enregistrer** pour enregistrer le projet.
11. Sélectionnez **Exporter > Package de provisionnement** pour créer un package à utiliser avec le provisionnement par lots, puis sélectionnez **Suivant**.
12. Enregistrez le **Mot de passe de chiffrement** pour une utilisation ultérieure dans le cas où vous souhaiteriez chiffrer le package, puis sélectionnez **Suivant**.
13. Enregistrez le package sur un lecteur USB pour le transférer vers chaque terminal à configurer. Vous pouvez également envoyer le package par e-mail sur le terminal.
14. Sélectionnez **Générer** pour créer le package.

Installer des packages de provisionnement

Après avoir créé les packages de provisionnement à l'aide de Microsoft Imaging and Configuration Designer, vous devez installer le package de provisionnement sur les terminaux des utilisateurs.

1. Sur le terminal à provisionner, accédez à **Paramètres** > **Comptes** > **Accès professionnel**, puis sélectionnez **Ajouter ou supprimer un package professionnel ou scolaire**. Si le package a été envoyé par e-mail, démarrez-le depuis votre client de messagerie.
2. Sélectionnez l'option **Ajouter un package** et sélectionnez **Média amovible** comme méthode pour ajouter le package.
3. Sélectionnez le package approprié dans la liste fournie.

   Si vous avez ajouté le terminal sur le compte de l'utilisateur dans Workspace ONE UEM console avant le provisionnement, le terminal est attribué au moment de l'enrôlement.

Enrôlement avec le Mode Enregistré

Les terminaux Windows enrôlés via VMware Workspace ONE Intelligent Hub ou OOBE sont gérés par défaut par MDM. Pour permettre aux terminaux Windows de s'enrôler sans gestion MDM, vous pouvez activer le Mode Enregistré (non géré) pour un groupe organisationnel entier ou avec des Smart Group et des critères spécifiques.

Le Mode Enregistré prend en charge les méthodes d'enrôlement répertoriées.

- Utilisateurs de préenrôlement
  - Préenrôlement de la ligne de commande
  - Préenrôlement manuel du terminal
  - Paramètres et valeurs de l'enrôlement silencieux
- Workspace ONE Intelligent Hub pour Windows avec authentification SAML

Activez le Mode Enregistré par groupes organisationnels ou par Smart Groups. Lorsque vous utilisez des Smart Groups, regroupez les terminaux pour le Mode Enregistré par version du système d'exploitation, plateforme, type de propriété ou utilisateurs.

Avec l'enrôlement en mode enregistré, les utilisateurs peuvent utiliser un sous-ensemble de services Workspace ONE sans la gestion MDM. Cela inclut Workspace ONE Assist, VMware Workspace ONE Tunnel, la gestion de l'expérience numérique des employés (DEEM) et les services Workspace ONE Hub.

Procédure

1. Dans Workspace ONE UEM console, sélectionnez le groupe organisationnel à activer avec l'enrôlement en mode Enregistré et accédez à **Terminaux** > **Paramètres du terminal** > **Terminaux et utilisateurs** > **Général** > **Enrôlement** > **Mode de gestion**.
2. Pour **Paramètre actuel**, sélectionnez **Remplacer**.
3. Pour **Windows**, sélectionnez **Activé**.
4. Sélectionnez **Activé** pour **Tous les terminaux Windows de ce groupe organisationnel**.
5. Si vous le souhaitez, vous pouvez ajouter des Smart Groups qui sont activés pour les

enrôlements en Mode Enregistré dans **Smart Groups Windows**.

6. Enregistrez vos paramètres.

Résultats

Les utilisateurs disposant de terminaux Windows enrôlés à partir du Smart Group configuré ou du groupe organisationnel spécifié peuvent utiliser les fonctionnalités du produit sans gestion MDM. Les informations sur le terminal et les capacités de gestion de la console sont limitées. Seuls les profils pertinents sont installés sur ces terminaux.

Paramètres d'intégration après enrôlement

Les administrateurs passent des flux de travail basés sur la création d'images au provisionnement juste-à-temps à distance. Dans ces scénarios de provisionnement, il est important d'informer les utilisateurs sur ce qui se passe lors de l'enrôlement de leurs terminaux.
VMware Workspace ONE Intelligent Hub pour Windows affiche et notifie les états des applications en cours de téléchargement et d'installation pendant le processus d'enrôlement Windows. Cette fonctionnalité permet également de personnaliser la messagerie utilisateur lors de la configuration.

Critères à prendre en compte

- Les paramètres d'intégration après l'enrôlement sont activés par défaut sur les terminaux Windows gérés dans Workspace ONE UEM.
- La fonctionnalité fonctionne dans Workspace ONE UEM version 2105 ou ultérieure.
- La fonctionnalité fonctionne avec VMware Workspace ONE Intelligent Hub pour Windows 21.05 et versions ultérieures.
- L'enrôlement par l'intermédiaire de VMware Workspace ONE Intelligent Hub pour Windows n'est pas requis, car cette fonctionnalité fonctionne pour n'importe quelle méthode d'enrôlement, notamment l'enrôlement Web. Cependant, vous devez installer l'application sur les terminaux pour appliquer les configurations et pour afficher l'expérience.

Comportements du VMware Workspace ONE Intelligent Hub

- Une fois installé, VMware Workspace ONE Intelligent Hub pour Windows détecte l'enrôlement et lance l'expérience.
  Remarque : L'expérience ne s'applique pas aux scénarios de mise à niveau. Cela n'affecte que les nouveaux enrôlements.
- Directement après l'enrôlement, VMware Workspace ONE Intelligent Hub lance et affiche vos personnalisations et suit toutes les applications définies pour un déploiement **Automatique**.

Désactiver l'expérience d'intégration après l'enrôlement

1. Sélectionnez le groupe organisationnel approprié.
2. Dans Workspace UEM Console, accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement > Invite facultative > Windows > Activer l'expérience d'intégration après l'enrôlement**.
3. Désactivez le paramètre.

Personnaliser le message d'expérience d'intégration après l'enrôlement

1. Sélectionnez le groupe organisationnel approprié.
2. Dans Workspace UEM Console, accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement > Invite facultative > Windows > Activer l'expérience d'intégration après l'enrôlement**.
3. Si cette fonctionnalité était précédemment désactivée, sélectionnez **Activé**. La fonctionnalité est activée par défaut.
4. Lorsque l'intégration après l'enrôlement est activée, vous pouvez personnaliser les champs **En-tête de bienvenue**, **Sous-en-tête de bienvenue** et **Texte du corps** du message d'expérience d'intégration après l'enrôlement à l'aide de valeurs de texte et de recherche.

États d'enrôlement Windows

Si vous examinez les paramètres d'enrôlement sur la page **Terminaux** > **Paramètres du terminal** > **Terminaux et utilisateurs** > **Général** > **Enrôlement**, vous voyez trois scénarios d'enrôlement généraux pour les terminaux Windows.

- **Enrôlement ouvert**

  Permet à toute personne répondant aux autres critères d'inscription (mode d'authentification, restrictions, etc.) de s'inscrire.

- **Terminaux enregistrés uniquement**

  Permet aux utilisateurs de s'inscrire à l'aide des terminaux enregistrés. L'enrôlement des terminaux correspond au processus d'ajout de terminaux professionnels dans Workspace ONE UEM console avant leur enrôlement. Cette matrice s'applique aux terminaux qui s'enregistrent sans jeton.

- **Exiger un jeton d'enregistrement**

  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.

Type de terminal

Le type de terminal détermine la manière dont le système Workspace ONE UEM suit et affiche l'état d'enrôlement du terminal.

- Terminaux sur liste autorisée : l'administrateur de Workspace ONE UEM ajoute une liste de terminaux pré-approuvés pour s'enrôler.
- Terminaux sur liste bloquée : l'administrateur de Workspace ONE UEM ajoute une liste de terminaux qui ne sont pas autorisés à s'enrôler.
- Terminaux enregistrés (sans attributs) : l'administrateur de Workspace ONE UEM enregistre les terminaux en ajoutant les informations sur le terminal à la console. Si l'administrateur n'entre pas les attributs du terminal, le système utilise les informations du terminal, notamment l'utilisateur, la plateforme, le modèle et le type de propriété.

- Terminaux enregistrés (avec attributs) : l'administrateur de Workspace ONE UEM enregistre les terminaux en ajoutant les attributs du terminal à la console. Les attributs du terminal comprennent l'UDID, l'IMEI et le numéro de série.

Cycle de vie de l'enrôlement des terminaux

L'enrôlement des terminaux avec Workspace ONE UEM se déroule en trois étapes principales.

1. (En option) Les administrateurs enregistrent les terminaux ou les utilisateurs enregistrent eux-mêmes leur terminal dans Workspace ONE UEM.

   L'enregistrement permet de limiter l'inscription.

2. Les utilisateurs ou les administrateurs enrôlent les terminaux avec Workspace ONE UEM.
3. Les utilisateurs ou les administrateurs désenrôlent les terminaux avec Workspace ONE UEM.

La console affiche les états SET.

Le type d'enrôlement, le type de terminal et l'étape d'enrôlement déterminent l'**État d'enrôlement** et l'**État du jeton** affichés pour les terminaux Windows sur la page **Terminaux** > **Cycle de vie** > **État d'enrôlement**.

Enrôlement ouvert

Type	Terminaux enregistrés : état d'inscription	Terminaux enregistrés : état du jeton	Terminaux inscrits : état d'inscription	Terminaux inscrits : état du jeton	Terminaux désinscrits : état d'inscription	Terminaux désinscrits : état du jeton
Terminal sur liste autorisée	Inscrit	Conforme	Enrôlé	Conforme	Désenrôlé	Conforme
Terminal sur liste bloquée	Sur liste bloquée	Non conforme	Non applicable	Non applicable	Non applicable	Non applicable
Terminal enregistré sans attributs. Les attributs sont le numéro de série, l'IMEI et l'UDID.	Inscrit	Inscription active	Enrôlé	Inscription active	Inscrit	Inscription active
Terminal enregistré avec attributs. Les attributs sont le numéro de série, l'IMEI et l'UDID.	Inscrit	Inscription active	Enrôlé	Inscription active	Inscrit	Inscription active

Terminaux enregistrés uniquement (pas de jeton)

Type	Terminaux enregistrés : état d'inscription	Terminaux enregistrés : état du jeton	Terminaux inscrits : état d'inscription	Terminaux inscrits : état du jeton	Terminaux désinscrits : état d'inscription	Terminaux désinscrits : état du jeton
Terminal sur liste autorisée	Inscrit	Conforme	Enrôlé	Conforme	Désenrôlé	Conforme
Terminal sur liste bloquée	Sur liste bloquée	Non conforme	Non applicable	Non applicable	Non applicable	Non applicable
Terminal enregistré sans attributs. Les attributs sont le numéro de série, l'IMEI et l'UDID.	Inscrit	Inscription active	Enrôlé	Inscription active	Inscrit	Inscription active

Type	Terminaux enregistrés : état d'inscription	Terminaux enregistrés : état du jeton	Terminaux inscrits : état d'inscription	Terminaux inscrits : état du jeton	Terminaux désinscrits : état d'inscription	Terminaux désinscrits : état du jeton
Terminal enregistré avec attributs. Les attributs sont le numéro de série, l'IMEI et l'UDID.	Inscrit	Inscription active	Enrôlé	Expiré	Inscrit	Inscription active

Exiger un jeton d'enregistrement

Type	Terminaux enregistrés : état d'inscription	Terminaux enregistrés : état du jeton	Terminaux inscrits : état d'inscription	Terminaux inscrits : état du jeton	Terminaux désinscrits : état d'inscription	Terminaux désinscrits : état du jeton
Terminal enregistré sans attributs. Les attributs sont le numéro de série, l'IMEI et l'UDID.	Inscrit	Inscription active	Enrôlé	Non applicable	Désenrôlé	Inscription expirée
Terminal enregistré avec attributs. Les attributs sont le numéro de série, l'IMEI et l'UDID.	Inscrit	Inscription active	Enrôlé	Non applicable	Désenrôlé	Inscription expirée

Enrôlement de terminaux pour la prise en charge multi-utilisateurs : Phase 1 (2210+)

La prise en charge multi-utilisateurs est une nouvelle fonctionnalité ajoutée à Workspace ONE UEM. Cette fonctionnalité permet à un utilisateur de se connecter à un PC enrôlé et de consulter ses échantillons et les détails des terminaux affichés dans la console. La prise en charge se déroulera par phases, avec la première phase commençant par l'enrôlement des terminaux via Azure Active Directory (ADD) et dans UEM. Les phases ultérieures seront étendues pour prendre en charge l'enrôlement basé sur un Hub sans aucune dépendance sur Azure Active Directory.

Présentation des fonctionnalités

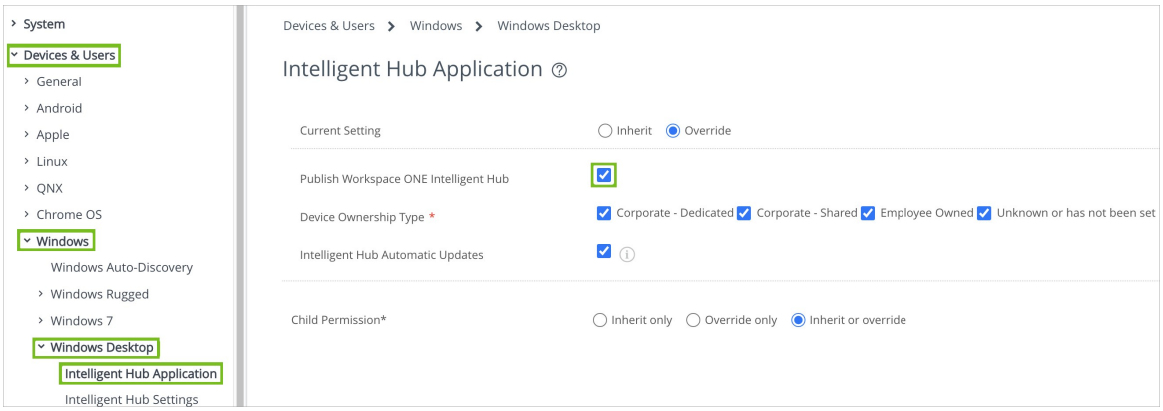
La première phase de cette fonctionnalité prendra en charge l'enrôlement des PC à l'aide de systèmes de l'environnement existant ayant réalisé l'expérience OOBE (Out-of-Box Experience) et disposant d'un administrateur local qui les joindra à AAD ou via OOBE pour les nouveaux environnements qui sont toujours en cours de configuration.

Les terminaux enrôlés de cette manière permettent à un utilisateur de se connecter à un PC enrôlé et de modifier l'attribution du PC à l'utilisateur actuel, ainsi que d'afficher les échantillons et les détails du terminal liés à l'utilisateur actuel dans la console.

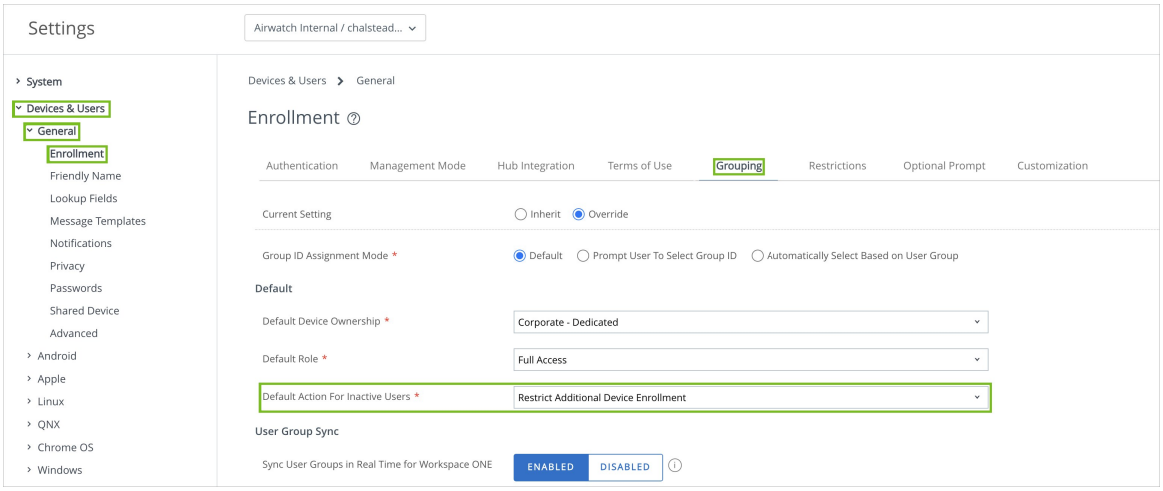
La prise en charge des ressources dans la phase 1 inclut les applications, les profils et les lignes de base. Cependant, les applications doivent être attribuées aux terminaux plutôt qu'aux utilisateurs afin d'empêcher les activités d'installation et de suppression d'applications en fonction de l'attribution des utilisateurs. D'autres ressources telles que les capteurs, les scripts et les flux de travail fonctionneront s'ils ciblent des groupes basés sur des terminaux. Les attributions basées sur l'utilisateur fonctionneront pour le premier utilisateur, mais pas pour les utilisateurs suivants. Les attributions basées sur l'utilisateur seront entièrement prises en charge pour tous les utilisateurs lors d'une phase ultérieure.

Exigences relatives à la version d'évaluation technique

- Le client est responsable des licences Azure AD Premium pour ses utilisateurs.
- L'environnement client doit être un locataire UeM SaaS 2209 ou version ultérieure sur le plan de contrôle.
- Intelligent Hub doit être publié depuis **Tous les paramètres** > **Terminaux et utilisateurs** > **Windows** > **Bureau Windows** > **Application Intelligent Hub**



- Intelligent Hub doit être de version 2206 ou ultérieure
- Un indicateur de fonctionnalité pour la prise en charge multi-utilisateurs doit être activé. L'équipe d'opérations VMware SaaS peut activer les indicateurs de fonctionnalités.
- L'intégration Azure AD doit être configurée dans UEM. Pour plus d'informations, reportez-vous à la section Paramètres des services d'annuaire.
- Les utilisateurs doivent enrôler le terminal à l'aide de la jonction AAD depuis un compte professionnel ou scolaire ou via le processus OOBE.
- Tous les utilisateurs du système doivent se connecter à l'aide d'informations d'identification AAD. Elles peuvent correspondre à un domaine personnalisé ou à un domaine Microsoft par défaut.
- Les utilisateurs doivent fermer leur session avant qu'un nouvel utilisateur ne se connecte. Le changement rapide d'utilisateur n'est pas pris en charge.
- Le paramètre pour **Terminaux et utilisateurs** > **Général** > **Enrôlement** > **Regroupement** > **Action par défaut pour les utilisateurs inactifs** doit être défini sur **Restreindre l'enrôlement de terminaux supplémentaires**.



Remarque : Si l'enregistrement du nouveau terminal demande d'ajouter un utilisateur, cela signifie que vous exécutez une version d'UEM antérieure à la version 2209 ou que l'indicateur de fonctionnalité peut ne pas être activé dans la version 2209. Pour utiliser cette fonctionnalité, vous devez demander que le paramètre « MultiUserPhase1EnrollmentSupportFeatureFlag » soit défini pour chaque groupe organisationnel dans lequel des terminaux multi-utilisateurs seront utilisés.

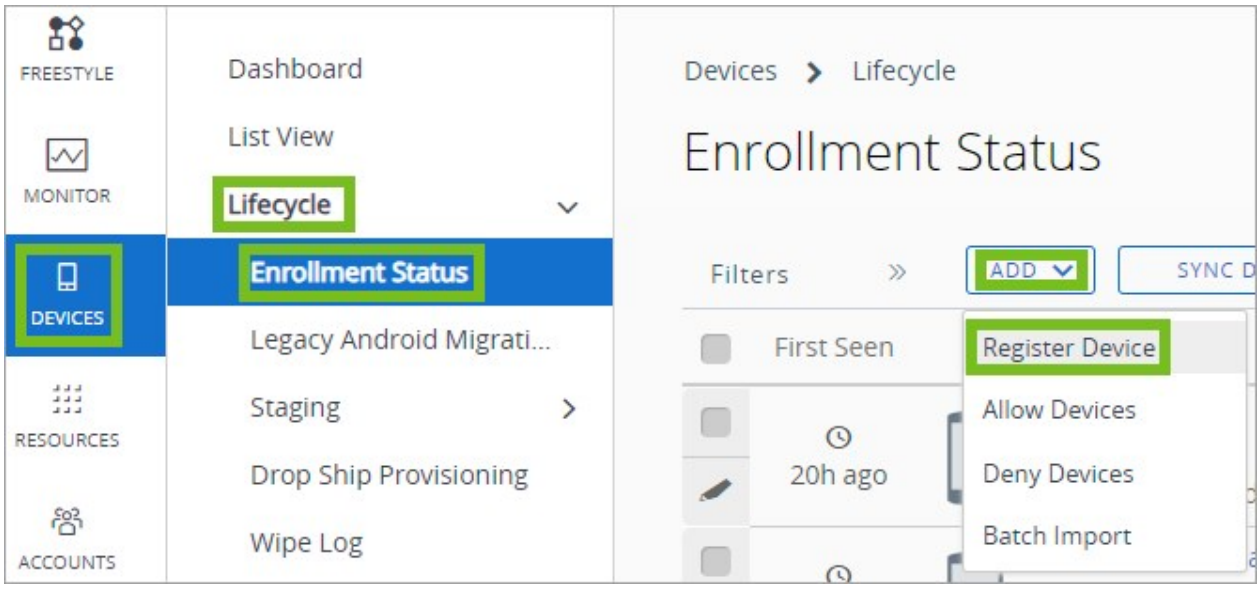
Remarque : Si l'enregistrement du nouveau terminal demande d'ajouter un utilisateur, cela signifie que vous exécutez une version d'UEM antérieure à la version 2209 ou que l'indicateur de

fonctionnalité peut ne pas être activé dans la version 2209. Pour utiliser cette fonctionnalité, vous devez demander que le paramètre « MultiUserPhase1EnrollmentSupportFeatureFlag » soit défini pour chaque groupe organisationnel dans lequel des terminaux multi-utilisateurs seront utilisés.

Enrôlement de systèmes multi-utilisateurs

L'enrôlement d'un système multi-utilisateurs commence par l'enregistrement du terminal. Le terminal ne doit pas avoir été enrôlé précédemment en tant que terminal unique. S'il a été précédemment enrôlé, l'enregistrement du terminal doit d'abord être supprimé de la console. Pour ce faire, accédez à la page des détails du terminal, choisissez plus d'actions, puis supprimez-le.

Avant l'enrôlement multi-utilisateurs, le terminal doit être enregistré dans le même groupe organisationnel que celui dans lequel l'intégration AAD est configurée. Accédez à **Terminaux** > **Cycle de vie** > **État d'enrôlement**, > choisissez **Ajouter** puis **Enregistrer le terminal**.

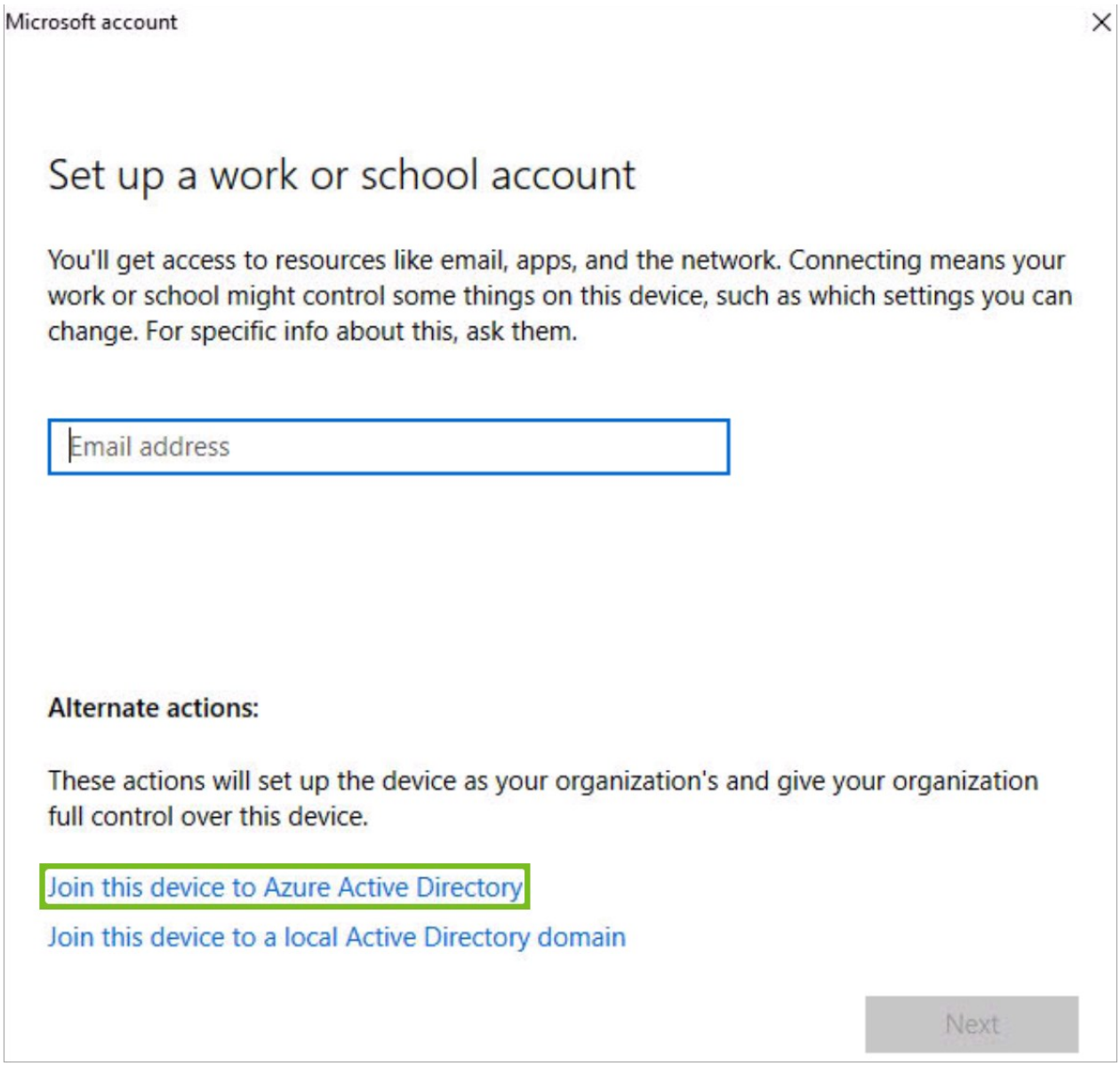


Le type de propriété doit être **Partagé par l'entreprise**, la plate-forme doit être **Windows Desktop** et le **Numéro de série** doit être renseigné.

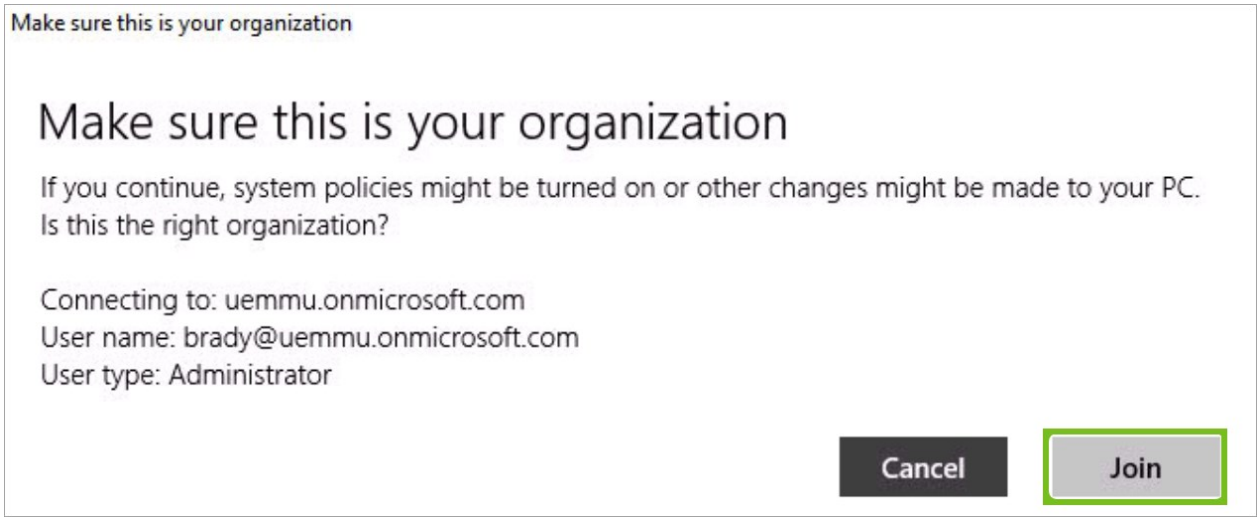
Flux d'enrôlement

Il existe deux options pour le processus d'enrôlement. La première option s'applique à un terminal qui est passé par OOBE et qui dispose d'un compte d'administrateur local configuré. La deuxième option s'applique à un terminal nouveau et qui n'est pas passé par OOBE.

Si le terminal est actuellement enregistré, est passé par OOBE et est actuellement connecté avec un compte d'administrateur local, procédez comme suit :
1. À partir du poste de travail d'un administrateur local, ouvrez **Paramètres > Comptes > Accès professionnel ou scolaire**.
2. Cliquez sur **Connecter**.
3. Au lieu de procéder à l'enrôlement lors de cette étape, sélectionnez l'option **Joindre ce terminal à Azure Active Directory**.



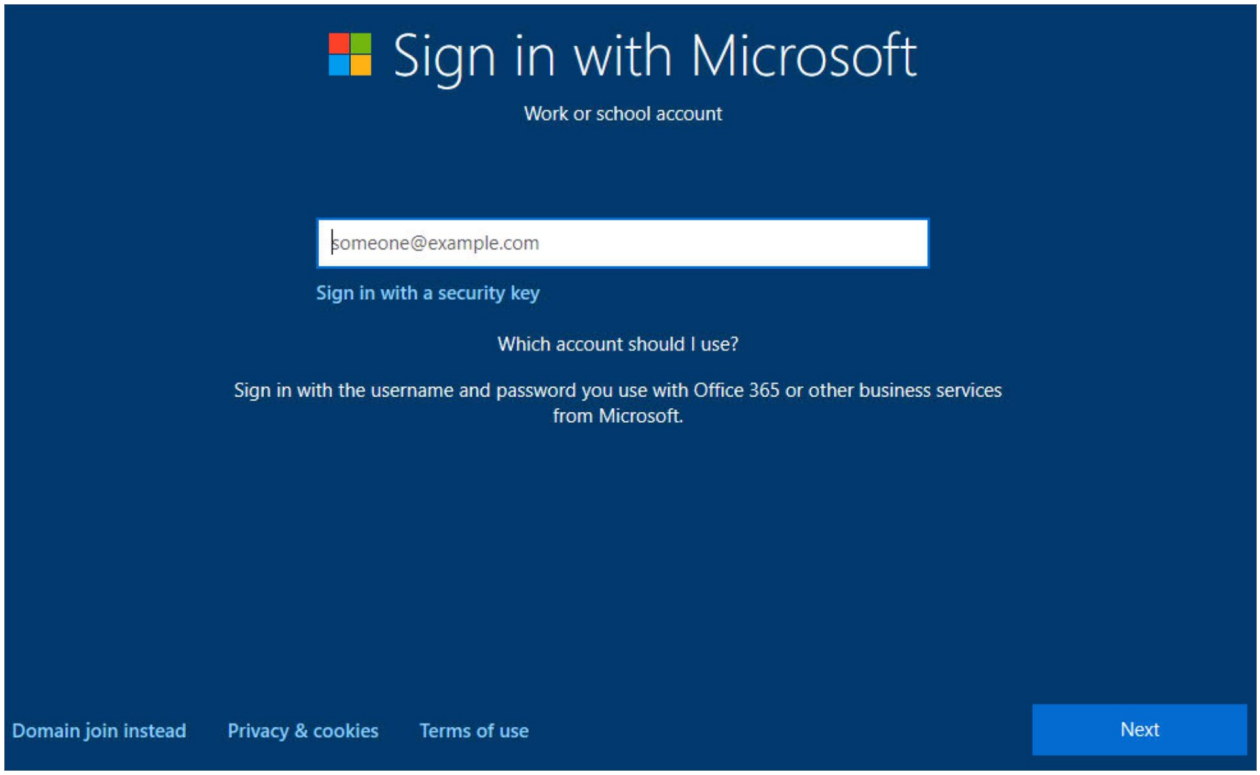
4 . Confirmez que les informations correctes sur l'organisation et l'utilisateur s'affichent. Terminez l'assistant de configuration de la jonction AAD à l'aide du compte d'un utilisateur dans le locataire AAD.



1. Une fois cette étape effectuée **déconnectez-vous** du compte local.

2. Ensuite, connectez-vous au PC à l'aide de vos informations d'identification AAD. *Notez que le premier utilisateur à se connecter au terminal sera un administrateur. Tous les utilisateurs supplémentaires seront des utilisateurs standard.*

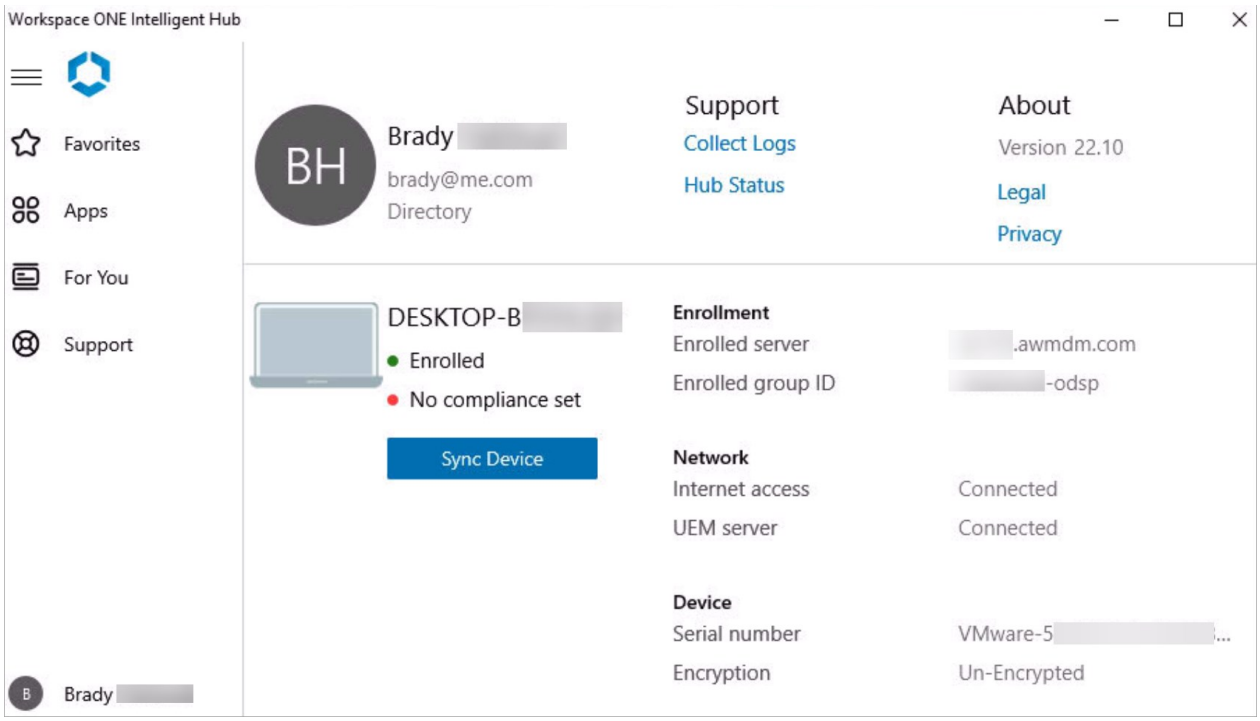
Si le terminal vient d'être déballé ou s'il n'est pas passé par le processus Out-of-Box Experience, procédez comme suit : 1. Dans la configuration OOBE de Windows, suivez les étapes de l'assistant jusqu'à ce que l'écran Se connecter avec Microsoft s'affiche. Un conseil : veillez à ce que l'heure du système soit exacte. Pour garantir cela, lorsque le terminal démarre dans OOBE, appuyez sur Maj-F10, puis forcez une synchronisation de l'heure à l'aide des commandes suivantes : *net start w32timew32tm /resync /force*



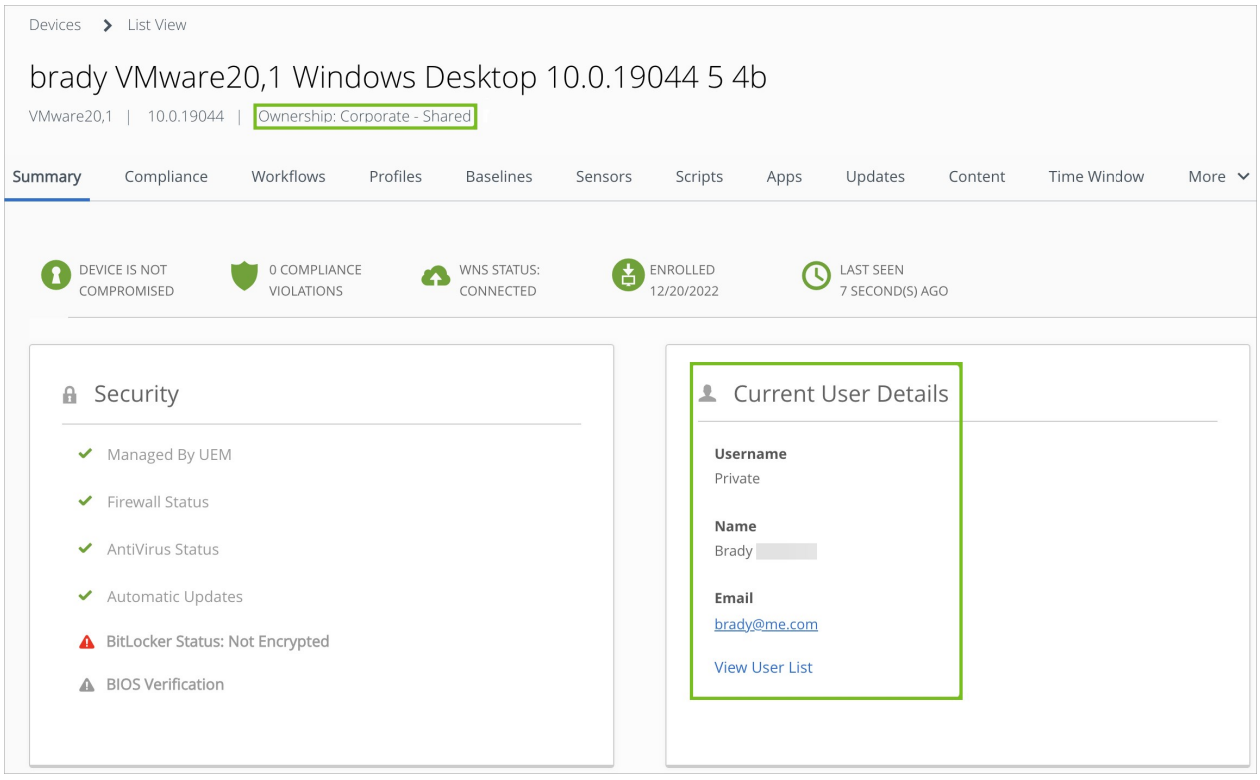
1. Saisissez les informations d'identification AAD de l'utilisateur qui sera l'administrateur du système. *Remarque : Par défaut, le premier utilisateur est Admin. Tous les utilisateurs supplémentaires seront des utilisateurs standard.*

Une fois le terminal enrôlé à l'aide de l'une de ces méthodes, Intelligent Hub est installé pour tous les utilisateurs. Vous devez activer l'option Publier le Hub via Paramètres > Terminaux et utilisateurs > Windows > Windows Desktop > Application Intelligent Hub.

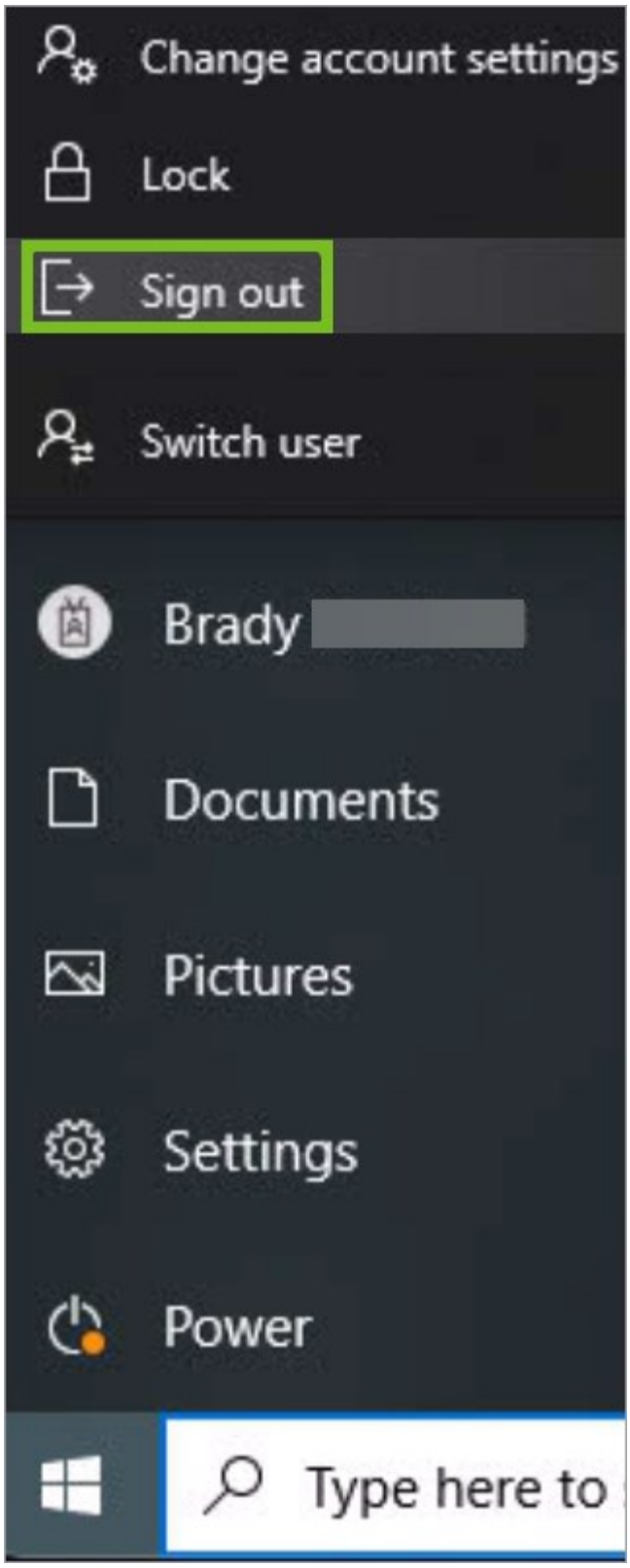
Lors du lancement du Hub, vous pouvez utiliser l'onglet Comptes pour vérifier que l'utilisateur du système correspond à l'utilisateur connecté.



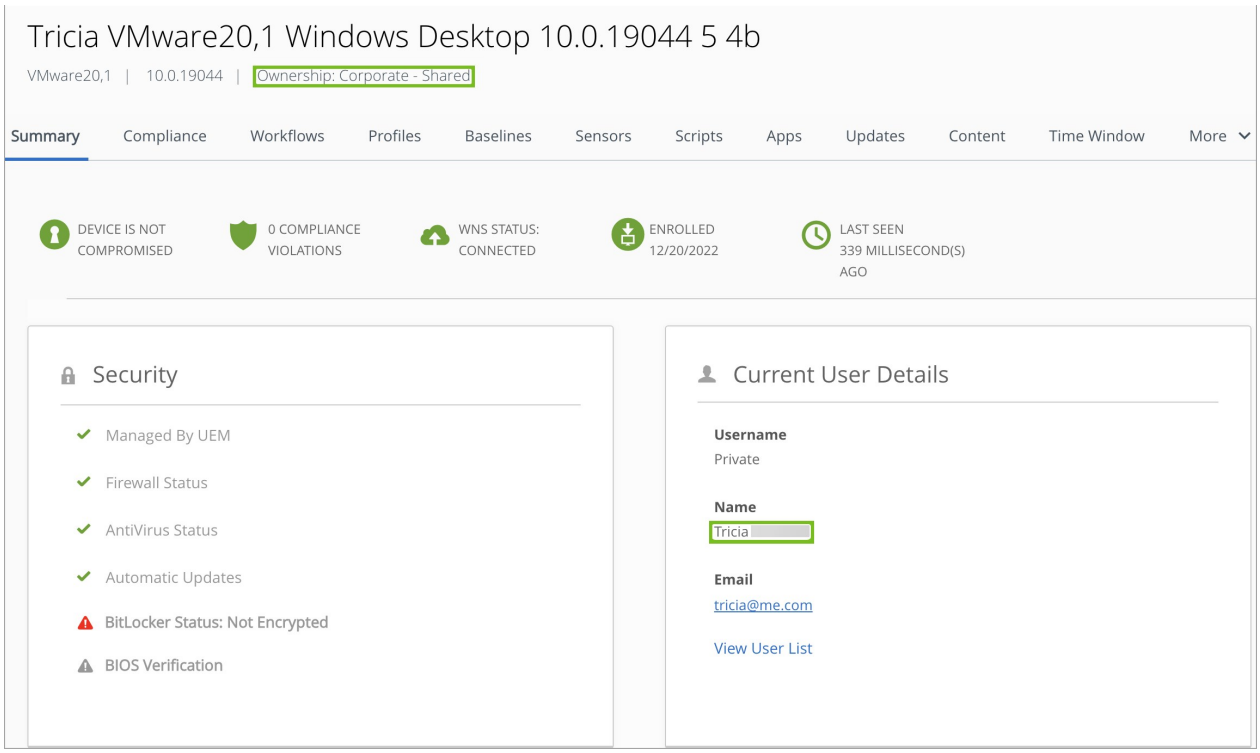
Vue de la console : Lorsque le premier utilisateur s'est connecté au poste de travail à l'aide de ses informations d'identification ADD, l'utilisateur doit être affiché en tant qu'utilisateur actuel dans la console. Le terminal doit être de type **Entreprise – Propriété partagée**.



Changement d'utilisateur : Déconnectez-vous du système et connectez-vous en tant qu'un autre utilisateur basé sur AAD pour finaliser le changement d'utilisateur.



Lors de la connexion au compte Active Directory Azure en tant qu'autre utilisateur, la page Compte Intelligent Hub affiche les détails de l'utilisateur actuel. Sur la console, la page **Détails du terminal** reflète le nouvel utilisateur.



Attributions de ressources

Applications natives : Les applications natives installées sur des systèmes multi-utilisateurs doivent être attribuées à des groupes intelligents basés sur les terminaux. Si elles sont attribuées à des groupes intelligents basés sur les utilisateurs, assurez-vous que tous les utilisateurs qui utiliseront le PC sont inclus dans l'attribution afin d'empêcher la suppression des applications lors du changement d'utilisateur.

Profils : Les profils peuvent être attribués à des utilisateurs ou à des terminaux. Les profils d'utilisateur et les profils de terminaux peuvent être attribués à des groupes intelligents basés sur des terminaux ou des utilisateurs.

FAQ

Le mode multi-utilisateurs sera-t-il uniquement pris en charge sur les environnements AAD ? Une phase ultérieure de développement ajoutera la prise en charge des environnements qui n'utilisent pas d'identités basées sur AAD.

Le mode multi-utilisateurs prendra-t-il en charge les enrôlements basés sur le Hub ? Une phase de développement future prendra en charge l'enrôlement basé sur le Hub via la ligne de commande/la prise en charge d'utilisateurs de préenrôlement.

Le mode multi-utilisateurs prendra-t-il en charge les annuaires LDAP non basés sur AD ? Le service informatique étudie la prise en charge des environnements qui utilisent LDAP ou d'autres annuaires à la place d'AD pour l'identité. Cela aura un impact sur les déploiements à un seul utilisateur et multi-utilisateurs.

Le mode multi-utilisateurs prendra-t-il en charge les environnements Windows multisession/Azure Virtual Desktop ? Une phase de développement future examinera la gestion basée sur AVD. L'ensemble des fonctionnalités prises en charge n'est pas connu à ce stade.

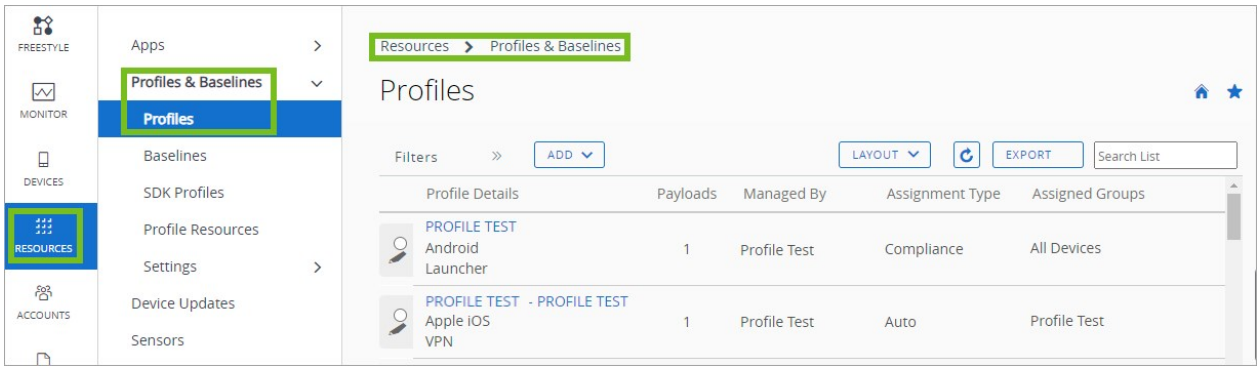
Profils Workspace ONE UEM pour Windows

Les profils dans Workspace ONE UEM sont les principaux moyens de gérer et de configurer vos terminaux Windows. Vous trouvez ici des informations sur différents profils qui se connectent aux ressources et les protègent, qui limitent et contrôlent les terminaux, et qui sont spécifiques à Dell.

Que sont les profils

Considérez les profils de sécurité comme des paramètres facilitant l'application des procédures de l'entreprise, lorsqu'ils sont combinés à des politiques de conformité. Ils contiennent les paramètres, les configurations et les restrictions que vous souhaitez appliquer aux terminaux.

Un profil est composé des paramètres de profil généraux et d'une section de configuration spécifique. Les profils fonctionnent mieux lorsqu'ils ne contiennent qu'une seule section de configuration. Dans la console Workspace ONE UEM, vous pouvez trouver des profils d'utilisateur et de terminal en accédant à : **Ressources** > **Profils et lignes de base** > **Profils**.



Niveau de l'utilisateur ou du terminal

Les profils Windows Desktop s'appliquent sur un terminal au niveau de l'utilisateur ou du terminal. Lors de la création de profils Windows Desktop, sélectionnez le niveau auquel s'applique le profil. Certains profils ne sont pas disponibles pour les deux niveaux. Vous pouvez uniquement les appliquer soit au niveau de l'utilisateur, soit au niveau du terminal. Workspace ONE UEM console identifie quels profils sont disponibles pour quel niveau. La liste suivante présente certaines mises en garde dont il faut tenir compte pour utiliser avec succès les profils de terminal et d'utilisateur.

- Workspace ONE UEM exécute les commandes qui s'appliquent au contexte du terminal, même si le terminal ne dispose d'aucune connexion active d'utilisateur enrôlé.
- Les profils d'utilisateur spécifiques requièrent une connexion active d'utilisateur enrôlé.

Vous pouvez utiliser certains profils et commandes standard pour configurer et contrôler le terminal. Le graphique ci-dessous montre les commandes pour le profil et la console qui n'ont plus besoin d'un utilisateur Windows actif pour les exécuter.

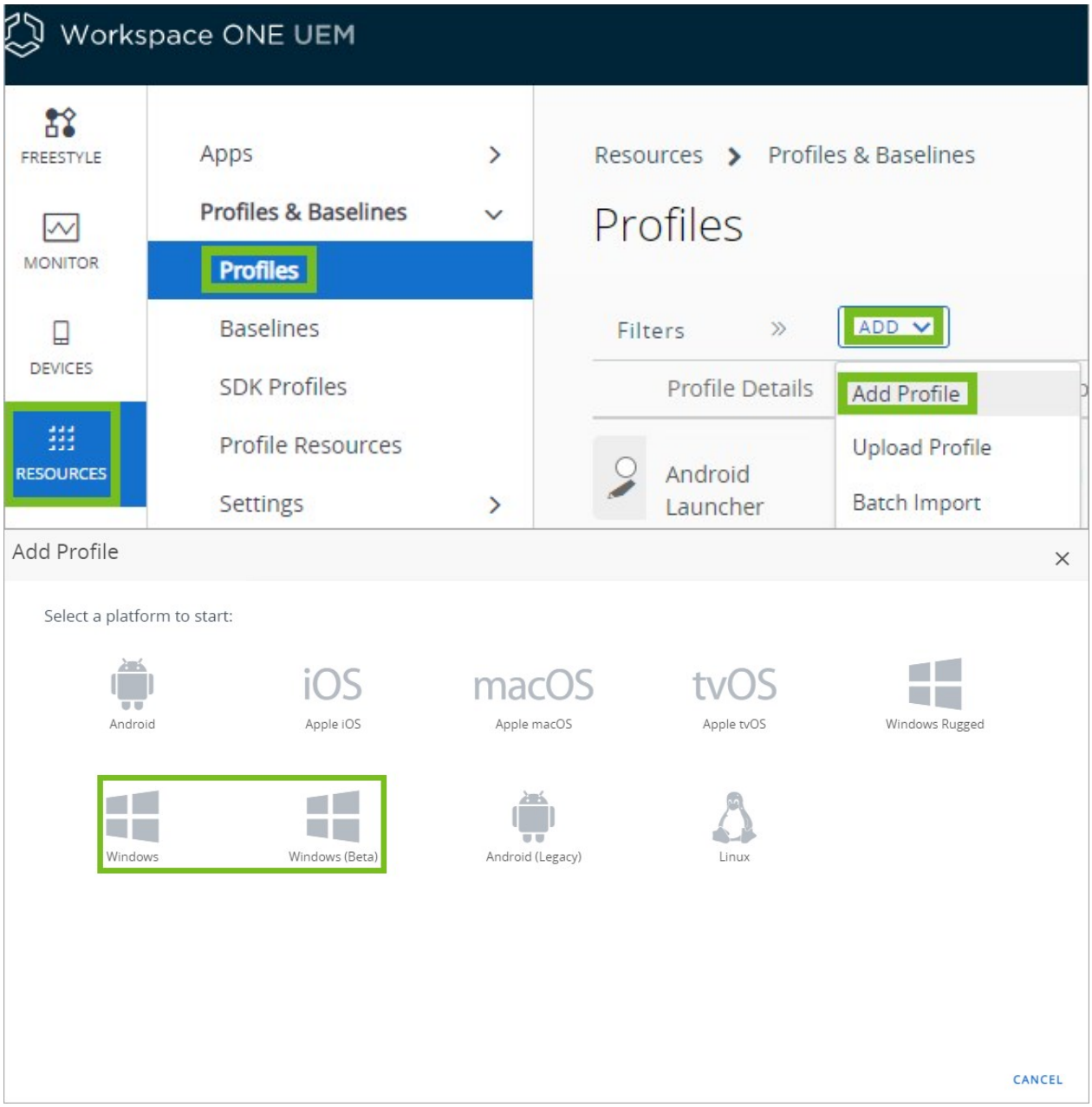
Nom de profil	Installe sans utilisateur Windows actif
Mot de passe	Oui
Wi-Fi	Oui
VPN	Oui
Identifiants	Oui
Restriction	Oui
Defender Exploit Guard	Oui
Protection des données	Oui
Windows Hello	Oui
Firewall	Oui
Chiffrements	Oui
Antivirus	Oui
Mises à jour Windows	Oui
Proxy	Oui
SCEP	Oui
Contrôle d'applications	Oui
Gestion des licences Windows	Oui
Profil personnalisé (HUB et OMA-DM)	Oui
Kiosque	Oui
Personnalisation	Oui
Distribution pair	Oui
Filtre d’écriture unifiée	Oui

Action de Console	Fonctionne sans utilisateur Windows actif
Sécurité des terminaux	Oui
Informations Windows	Oui
Attestation d'intégrité	Oui
Mises à jour du système d'exploitation disponibles	Oui
Check-in du Hub	Oui
Exemple de liste de certificats	Oui
Informations de sécurité	Oui
Informations	Oui
Exemple de liste d'applications - HUB	Oui

Action de Console	Fonctionne sans utilisateur Windows actif
Exemple de liste d'applications - OMA-DM	Oui
Capteur	Oui
Flux de travail	Oui
Fenêtre de temps	Oui
Redémarrage	Oui
Effacement des données professionnelles	Oui
Réinitialisation du terminal	Oui
Réinitialisation des données d'entreprise	Oui
Demander la journalisation du terminal	Oui

Nouvelles options de profil pour la configuration des profils d'utilisateurs et de terminaux Windows

Nous avons mis à jour vos options d'attribution des profils d'utilisateurs et de terminaux en ajoutant un deuxième générateur de plateforme Windows(bêta). Dans la console, lors de l'ajout d'un profil d'utilisateur ou de terminal, vous devrez sélectionner les plateformes Windows ou Windows(bêta). Navigation : **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Windows -OU- Windows(bêta)**

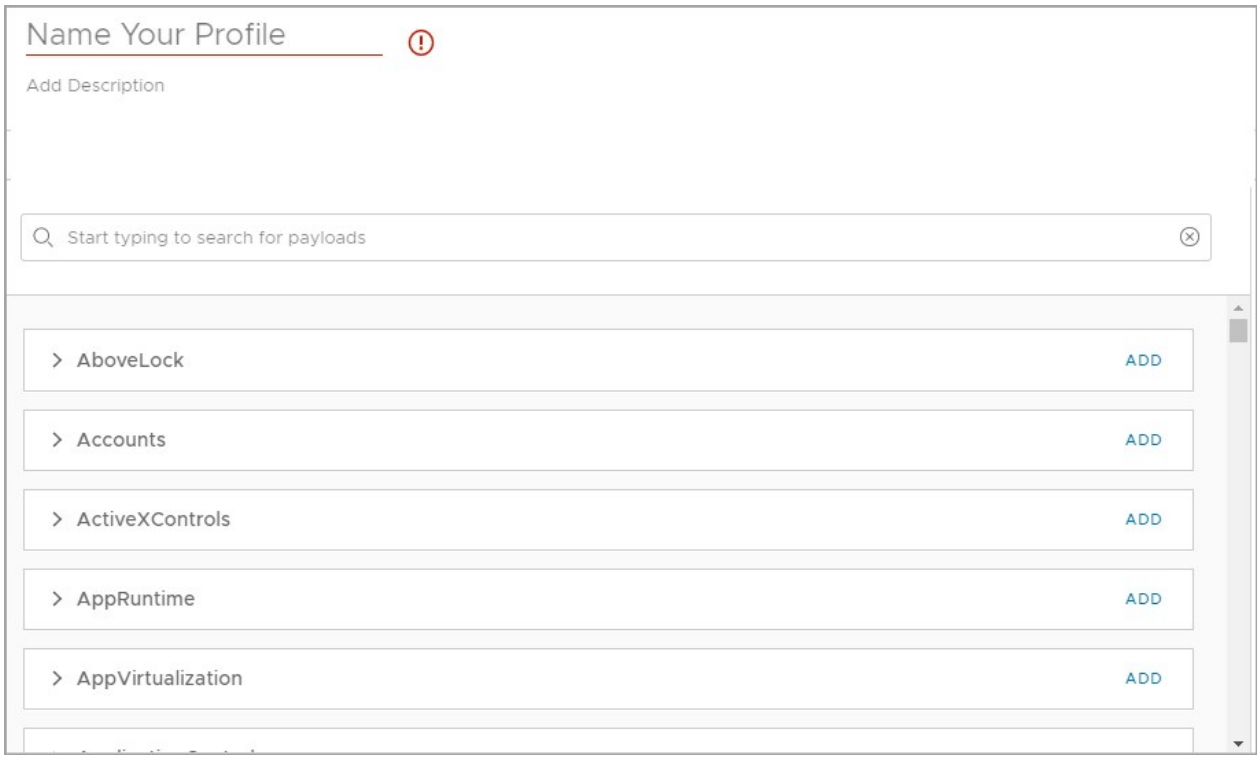


Option de plateforme Windows

Vous pouvez continuer à ajouter et personnaliser des profils d'utilisateurs et de terminaux avec des paramètres personnalisés et l'intégration à Workspace ONE Intelligent Hub à l'aide de cette option de plateforme. Si vous avez configuré des paramètres personnalisés via l'Intelligent Hub, continuez à utiliser cette option au lieu de migrer vers les nouvelles options de plate-forme Windows(bêta), car la version bêta ne prendra pas en charge tous les paramètres personnalisés pour le moment.

Option de plateforme Windows(bêta)

Migrez vers cette plateforme si vous n'utilisez pas de paramètres personnalisés pour vos profils d'utilisateurs et de terminaux. Lors de l'ajout d'un profil, vous pourrez rechercher les options de fournisseurs de services de configuration natifs (CSP) Microsoft, puis l'appliquer à vos profils si nécessaire. Les améliorations ultérieures seront apportées, telles que l'ajout de modèles VMware actuellement définis sur un indicateur de fonctionnalité.

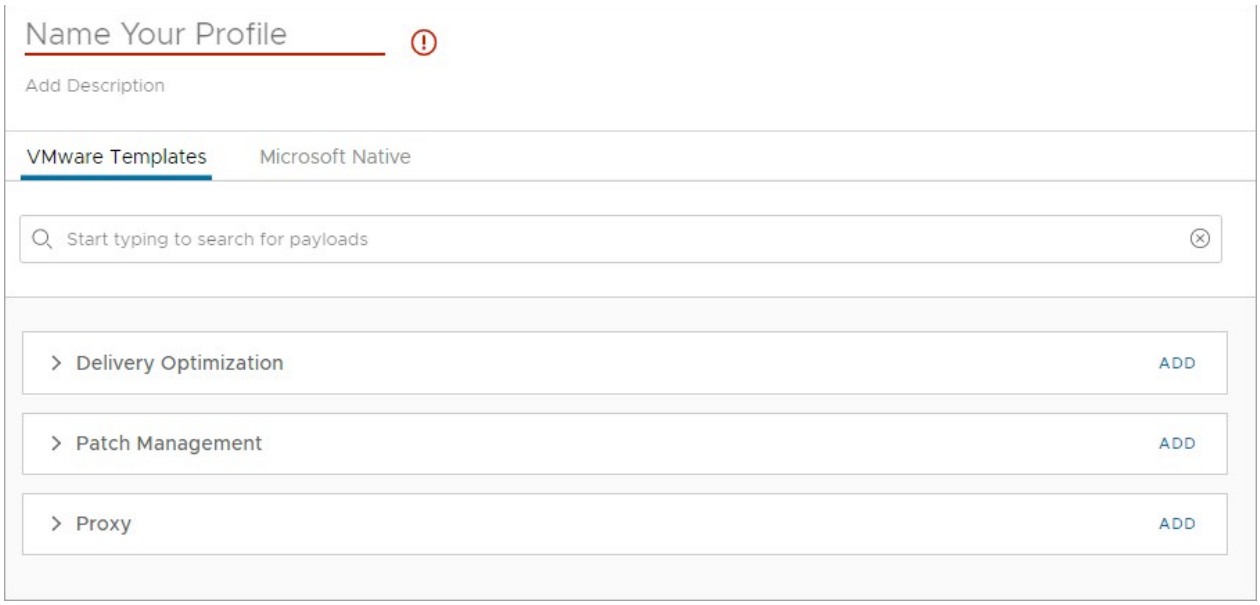


Les paramètres personnalisés ne sont actuellement pas pris en charge. Une liste complète des détails des CSP est disponible sur le site web de Microsoft : https://msdn.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider.

Indicateur de fonctionnalité - Modèles VMware

Sous l'option de plateforme Windows(bêta) et derrière un indicateur de fonctionnalité, nous avons créé des modèles VMware DDUI (Data-Driven User Interface). Vous remarquerez qu'il existe deux onglets dans la console, **Modèles VMware** et **Microsoft Natif**. L'onglet Modèles VMware offre aux administrateurs des options plus granulaires pour définir un niveau de personnalisation plus approfondi de certains CSP natifs Microsoft avec des paramètres préconfigurés et la possibilité de personnaliser trois de nos configurations les plus courantes sous : Optimisation de la distribution, Gestion des correctifs et Proxy. À l'aide des options dans ces sections, vous pouvez ajuster les paramètres préconfigurés selon vos besoins.

Ensuite, l'onglet **Microsoft Natif** permet toujours de rechercher et d'appliquer d'autres options de CSP natifs Microsoft si nécessaire. **Remarque :** Si vous configurez les deux onglets, assurez-vous que les éléments dans les modèles VMware ne sont pas également définis sous le Microsoft natif, car l'un d'eux peut remplacer l'autre et/ou créer un problème.

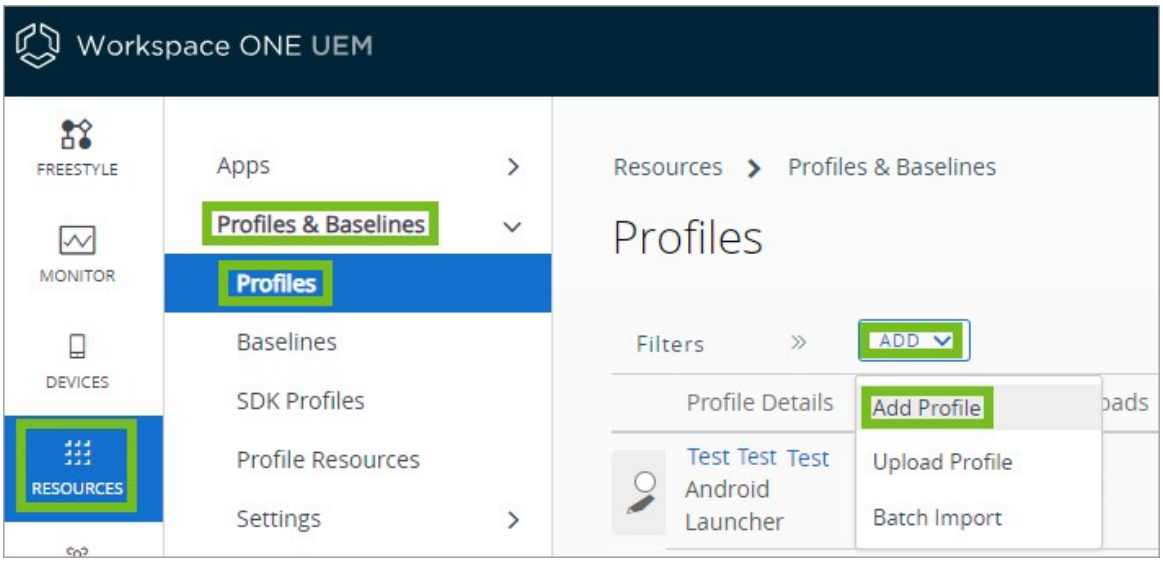


Profil d'antivirus

La création d'un profil d'**antivirus** permet de configurer l'antivirus Windows Defender natif sur les terminaux Windows Desktop. Le fait de configurer Windows Defender pour tous les terminaux permet de garantir la protection des utilisateurs utilisant leur terminal.

Important : Ce profil ne configure que l'Antivirus Windows Defender natif, pas les autres programmes antivirus tiers.

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



2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Antivirus**.
6. Configurez les paramètres dans l'onglet **Antivirus** :

Paramètres	Descriptions
Surveillance en temps réel	Activez ce paramètre pour que l'Antivirus Windows Defender surveille le terminal en temps réel.
Sens d'analyse en temps réel	Activez ce paramètre pour que l'Antivirus Windows Defender surveille les fichiers entrants, les fichiers sortants ou tous les fichiers. Utilisez cette option pour obtenir des performances réseau pour les serveurs ou les rôles de serveur que vous avez définis pour les installations Windows Server qui gèrent le trafic dans un sens unique.
Niveau de protection du cloud	Activez ce paramètre pour configurer le degré d'agressivité de l'Antivirus Windows Defender en matière de blocage et d'analyse des fichiers suspects. Prenez en considération les performances réseau lors de la configuration de cet élément de menu.
Délai d'expiration du bloc du cloud	Sélectionnez une durée, en secondes, pendant laquelle un fichier reste bloqué lorsque l'Antivirus Windows Defender analyse son potentiel de menace. La durée de blocage par défaut est de 10 secondes. Le système ajoute les secondes définies dans cet élément de menu à la durée par défaut.
Mises à jour de la signature	Intervalle de mise à jour de la signature en heures Sources des partages de fichiers des mises à jour de la signature Vérifier la signature avant l'exécution de l'analyse Ordre de rétablissement des mises à jour de la signature
Intervalle d'analyse	**Analyse complète** : activez ce paramètre pour planifier une analyse complète. Sélectionnez l'intervalle de temps (en heures) entre les analyses. **Analyse rapide** : activez ce paramètre pour planifier une analyse rapide. Sélectionnez l'intervalle de temps (en heures) entre les analyses.
Exclusions	Sélectionnez les chemins de fichier ou processus à exclure des analyses de l'Antivirus Windows Defender. Sélectionnez **Ajouter nouveau** pour ajouter une exception.
Action par défaut contre les menaces (Basse, Modérée, Haute, Grave)	Définissez l'action par défaut pour les niveaux de menaces différentes rencontrés durant les analyses. **Effacer** – Sélectionnez ce paramètre pour effacer les problèmes inhérents à la menace. **Quarantaine** – Sélectionnez ce paramètre pour isoler la menace dans un dossier de quarantaine. **Supprimer** – Sélectionnez ce paramètre pour supprimer la menace de votre système. **Autoriser** – Sélectionnez ce paramètre pour conserver la menace. **Personnalisé** – Sélectionnez ce paramètre pour laisser l'utilisateur choisir l'action qu'il souhaite entreprendre sur la menace. **Aucune action** – Sélectionnez ce paramètre pour n'entreprendre aucune action sur la menace. **Bloquer** – Sélectionnez ce paramètre pour bloquer la menace et l'empêcher d'accéder au terminal.
Avancé	**Analyser le facteur de charge CPU moyen** : définissez le pourcentage moyen maximal du processeur que l'Antivirus Windows Defender peut utiliser au cours des analyses. **Verrouillage IU** : activez ce paramètre pour verrouiller intégralement l'interface utilisateur de sorte que les utilisateurs finaux ne puissent pas modifier de paramètres. **Analyse complète de rattrapage** : activez ce paramètre pour autoriser l'exécution d'une analyse complète ayant été précédemment interrompue ou manquée. Une analyse de rattrapage est entreprise lorsqu'une analyse planifiée n'a pas pu être effectuée. En règle générale, la non-exécution d'analyses régulières est due au fait que l'ordinateur était éteint à ce moment-là. **Analyse rapide de rattrapage** : activez ce paramètre pour autoriser l'exécution d'une analyse rapide ayant été précédemment interrompue ou manquée.

Paramètres	Descriptions
	Une analyse de rattrapage est entreprise lorsqu'une analyse planifiée n'a pas pu être effectuée. En règle générale, la non-exécution d'analyses régulières est due au fait que l'ordinateur était éteint à ce moment-là. **Analyse du comportement** : activez ce paramètre pour que l'analyseur de virus envoie un journal d'activité à Microsoft. **Système de prévention d'intrusion** : activez ce paramètre pour configurer la protection du réseau contre l'exploitation de vulnérabilités connues. Cette option permet à l'Antivirus Windows Defender de surveiller les connexions en permanence et d'identifier les comportements potentiellement malveillants. À cet égard, le logiciel se comporte tel un analyseur de virus classique, mais au lieu d'analyser des fichiers, il analyse le trafic réseau. **Protection PUA** : activez ce paramètre pour que l'Antivirus Windows Defender surveille les applications potentiellement indésirables (PUA) sur les clients finaux. **Protection IOAV** : activez ce paramètre pour que Windows Defender analyse les fichiers téléchargés. **Protection OnAccess** : activez ce paramètre pour que l'Antivirus Windows Defender protège les fichiers et les dossiers contre tout accès non autorisé. Protection du Cloud : activez ce paramètre pour que l'Antivirus Windows Defender détecte et empêche les menaces rapidement à l'aide des ressources propriétaires et l'apprentissage machine. **Consentement de l'utilisateur** : activez ce paramètre pour que l'Antivirus Windows Defender invite l'utilisateur du client final à donner son consentement avant qu'il agisse sur les menaces identifiées. **Analyse des e-mails** : activez ce paramètre pour que Windows Defender analyse les e-mails. **Analyser les lecteurs réseau mappés** : activez ce paramètre pour que l'Antivirus Windows Defender analyse des lecteurs mappés vers des terminaux. **Analyser les archives** : activez ce paramètre pour que l'Antivirus Windows Defender exécute une analyse complète sur des dossiers archivés. **Analyser les lecteurs amovibles** : activez ce paramètre pour que l'antivirus Windows Defender analyse tout lecteur amovible rattaché au terminal. **Supprimer les fichiers en quarantaine après** : définissez la durée de conservation des fichiers placés en quarantaine avant leur suppression.

7. Cliquez sur **Enregistrer et publier**.

Profil de contrôle d’applications

Limitez les applications pouvant être installées sur les terminaux Windows Desktop avec le profil Contrôle des applications. Le fait de limiter les installations d'applications protège vos données des applications malveillantes et évite aux utilisateurs de recevoir sur les terminaux de l'entreprise des applications dont ils n'ont pas besoin.

Pour autoriser ou interdire l'installation d'applications sur les terminaux, activez le contrôle des applications pour approuver ou bloquer des applications spécifiques. Alors que le moteur de conformité surveille les terminaux et y recherche les applications approuvées ou bloquées, le contrôle des applications empêche les utilisateurs d'essayer d'ajouter ou de supprimer des applications. Vous pouvez, par exemple, empêcher l'installation de certaines applications de jeux ou autoriser seulement les applications approuvées. Les applications bloquées et installées sur un terminal avant l'envoi de la section de configuration Contrôle des applications sont désactivées une fois le profil déployé.

Le profil Contrôle d'application réduit le coût de gestion des terminaux, car il empêche l'utilisateur d'exécuter des applications interdites qui pourraient provoquer des problèmes. Le blocage des applications pouvant provoquer des problèmes réduit le nombre d'appels auxquels le personnel d'assistance doit répondre.

Configuration d'un profil Contrôle des applications

Activez le contrôle des applications pour approuver ou bloquer des applications spécifiques pour autoriser ou interdire l'installation d'applications sur les terminaux. Le contrôle des applications utilise des configurations Microsoft AppLocker pour forcer le contrôle des applications sur les terminaux Windows.

Pour configurer un fichier de configuration XML, vous devez configurer les paramètres Applocker sur un terminal et exporter le fichier à utiliser avec le profil.

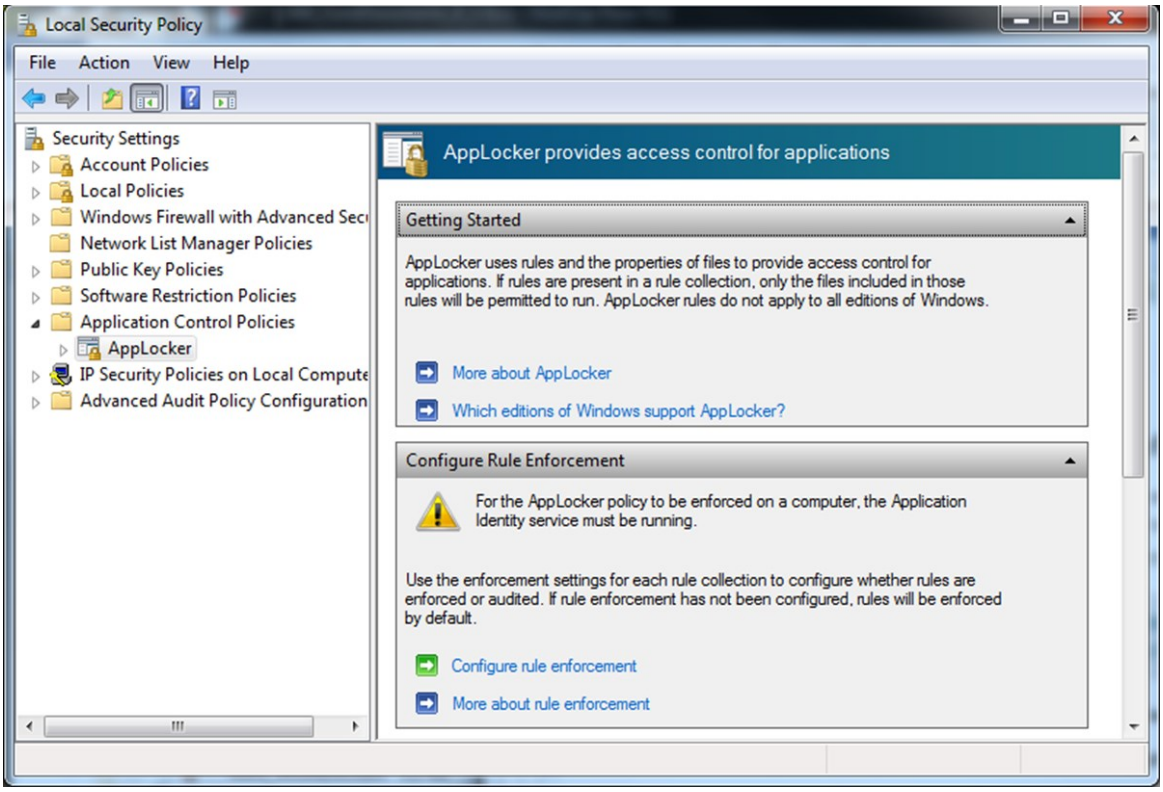
Le profil Contrôle des applications requiert Windows Entreprise ou Éducation.

Important :

- Créez d'abord des politiques à l'aide du mode Auditer uniquement. Après avoir vérifié la version configurée à l'aide du mode Auditer uniquement sur un terminal de test, créez une version en mode Appliquer que vous utiliserez sur vos terminaux. Si vous ne testez pas les politiques avant une utilisation générale, vous risquez de rendre vos terminaux inutilisables.
- Créez des règles par défaut et toute autre règle nécessaire pour votre organisation afin de réduire les risques de verrouillage des configurations par défaut ou de bloquer les terminaux après le redémarrage. Pour savoir comment créer des règles, voir l'article de Microsoft TechNet article sur AppLocker.

Procédure

1. Sur le terminal de configuration, lancez l'éditeur **Stratégie de sécurité locale**.
2. Naviguez vers **Stratégies de contrôle de l'application** > **AppLocker**, puis sélectionnez **Configurer la mise en application des règles**.



3. Activez **Règles de l'exécutable**, **Règles Windows Installer**, puis la mise en application **Règles de script** en sélectionnant **Appliquer les règles**.
4. Créez des **Règles de l'exécutable**, des **Règles Windows Installer** et des **Règles de script** en sélectionnant le dossier sur la droite, en effectuant un clic droit sur le dossier et en choisissant **Créer Nouvelle règle**. N'oubliez pas de créer des règles par défaut afin de réduire les risques de verrouillage de la configuration par défaut ou le blocage du terminal.
5. Une fois toutes les règles requises créées, effectuez un clic droit sur **AppLocker**, sélectionnez **Exporter la stratégie**, puis enregistrez le fichier de configuration XML.
6. Dans Workspace ONE UEM Console, accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**, puis sélectionnez **Ajouter un profil**.
7. Sélectionnez **Windows**, puis **Windows Desktop**.
8. Sélectionnez **Profil de terminal**.
9. Configurez les **paramètres généraux** du profil.
10. Sélectionnez la section de configuration **Contrôle d'applications**.
11. Sélectionnez **Importer un modèle de configuration de terminaux**, puis **Importer** pour ajouter votre **fichier de configuration des politiques**.
12. Cliquez sur **Enregistrer et publier**.

Profil BIOS

Configurez les paramètres BIOS pour des terminaux Dell Enterprise à l'aide du profil BIOS. Ce profil nécessite l'intégration à Dell Command | Monitor.

La prise en charge des paramètres de profil BIOS varie selon le terminal Dell Enterprise. Dell

Command | Monitor doit être chargé et/ou attribué à chaque terminal.

Conditions prérequises

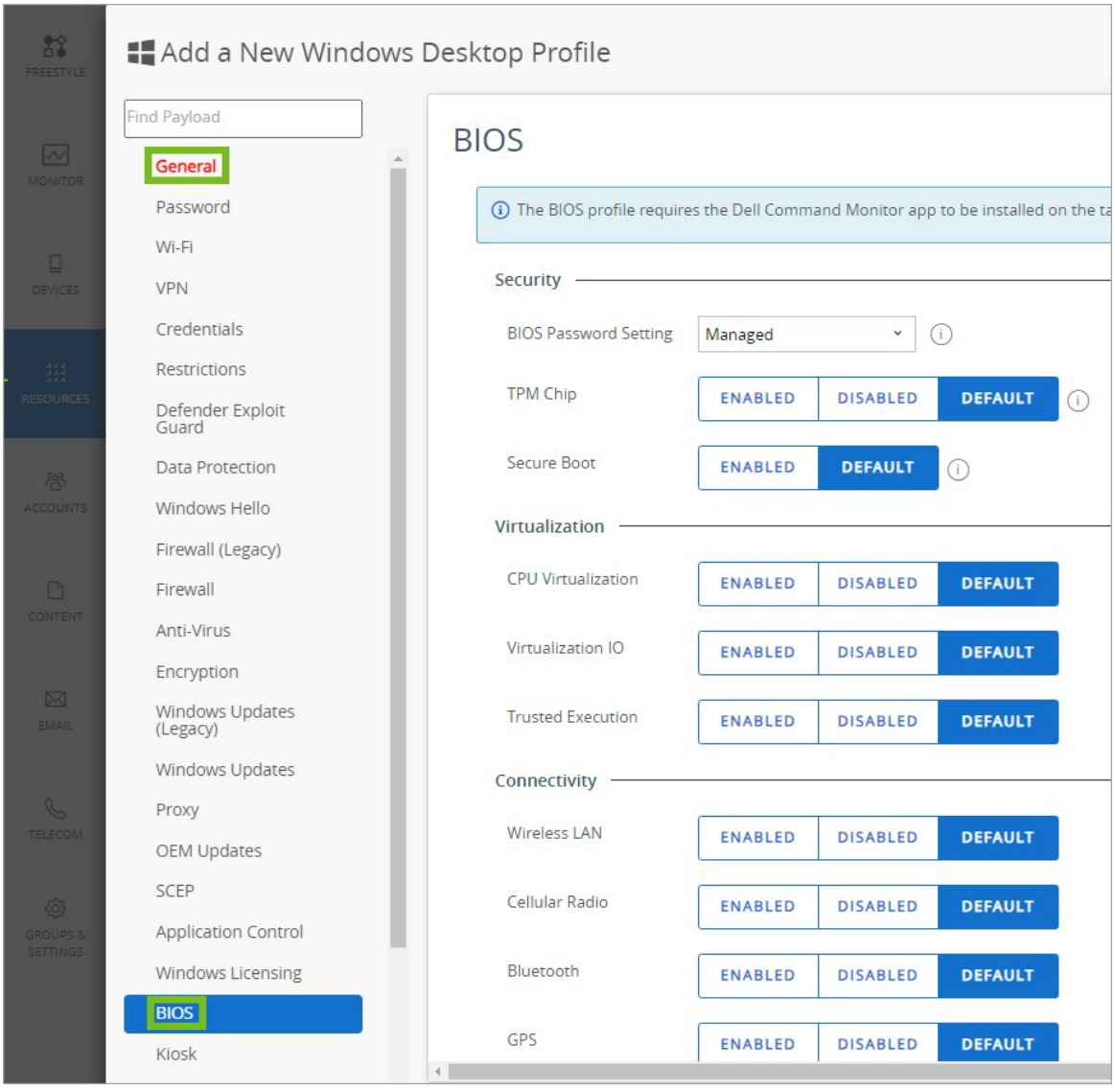
- Si vous souhaitez utiliser la fonctionnalité de module de configuration, vous devez déployer l'application Dell Command | Configure sur les terminaux.
- Ce profil nécessite également l'intégration à Dell Command | Monitor. Ajouter Dell Command | Products.

Procédure

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.

Remarque : Il existe désormais une option par défaut pour les profils. L'option par défaut n'apportera aucune modification au paramètre sur le terminal. Dans les paramètres par défaut du nouveau profil, les paramètres de mot de passe seront définis sur **Gérer** et tous les autres paramètres seront définis sur **Par défaut**.

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



2. Sélectionnez la section de configuration **BIOS** et configurez les paramètres suivants.
    - **Définition du mot de passe du BIOS** : sélectionnez **Géré** pour que Workspace ONE UEM génère automatiquement un mot de passe du BIOS unique et fiable pour les terminaux. Vous pouvez accéder au mot de passe généré sur la page Détails du terminal. Sélectionnez **Manuel** pour entrer votre propre mot de passe du BIOS.
    - **Mot de passe du BIOS** : entrez le mot de passe utilisé pour déverrouiller le BIOS du terminal. Ce paramètre s'affiche lorsque le **paramètre de mot de passe du BIOS** est défini sur Manuel.
    - **Puce du TPM** : sélectionnez **Activer** pour activer la puce du Module de plateforme sécurisée (TPM). Si vous désactivez la puce du TPM, vous désactivez également la capacité de mot de passe à usage unique du BIOS. Le mot de passe du BIOS défini dans le profil du BIOS géré ne change pas après utilisation.
    - **Démarrage sécurisé** : sélectionnez **Activer** pour utiliser les paramètres de démarrage sécurisé sur le terminal. Vous ne pouvez pas désactiver le démarrage sécurisé avec DCM.
    - **Virtualisation du processeur** : sélectionnez **Activer** pour autoriser la prise en charge de la virtualisation du matériel.
    - **Virtualisation IO** : sélectionnez **Activer** pour autoriser la virtualisation d'entrée/de sortie
    - **Trusted Execution** : sélectionnez **Activer** pour autoriser le terminal à utiliser la puce TPM, la virtualisation CPU et la virtualisation IO pour les décisions de confiance. Pour utiliser la fonctionnalité Trusted Execution, vous devez définir les paramètres **Puce TPM**, **Virtualisation CPU** et **Virtualisation IO** sur **Activé**.
    - **Réseau local sans fil** : sélectionnez **Activer** pour autoriser l'utilisation de la fonctionnalité LAN sans fil du terminal.
    - **Radio cellulaire** : sélectionnez **Activer** pour autoriser l'utilisation de la fonctionnalité Radio cellulaire du terminal.
    - **Bluetooth** : sélectionnez **Activer** pour autoriser l'utilisation de la fonctionnalité Bluetooth du terminal.
    - **GPS** : sélectionnez **Activer** pour autoriser l'utilisation de la fonctionnalité GPS du terminal.
    - **Rapports SMART** : sélectionnez **Activer** pour utiliser les rapports SMART des solutions de stockage du terminal
    - **Charge de la batterie principale** : sélectionnez les règles de chargement pour le terminal. Ces règles contrôlent le démarrage et l'arrêt de la charge de la batterie. Si vous sélectionnez **Charge personnalisée**, vous pouvez définir manuellement le pourcentage de charge pour le démarrage et l'arrêt de la charge de la batterie.
        - Charge standard – Utilisez cette option pour les utilisateurs qui basculent entre fonctionnement sur batterie et sur source d'alimentation externe. Cette option charge entièrement la batterie à un taux standard. Le temps de charge varie selon le modèle de terminal.

- Charge Express – Utilisez cette option pour les utilisateurs qui ont besoin de charger la batterie sur une courte période. La technologie de charge rapide de Dell permet de charger une batterie complètement déchargée à 80 % en environ 1 heure lorsque l'ordinateur est mis hors tension et à 100 % en environ 2 heures. Le temps de charge peut être plus long si l'ordinateur est allumé.
- Charge CA – Utilisez cette option pour les utilisateurs qui emploient principalement leur système lorsqu'ils sont connectés à une source d'alimentation externe. Ce paramètre peut prolonger la durée de vie de votre batterie en diminuant le seuil de charge.
- Charge automatique – Utilisez cette option pour les utilisateurs qui souhaitent définir cette option et ne plus en changer. Cette option permet au système d'optimiser les paramètres de votre batterie en fonction des habitudes d'utilisation de la batterie.
- Charge personnalisée – Utilisez cette option pour les utilisateurs avancés qui souhaitent plus de contrôle sur la charge et la décharge de leur batterie.

- **Limite de début de charge personnalisé de la batterie principale** : définissez le pourcentage de charge de la batterie qui doit être atteint avant que le terminal commence à charger la batterie.
- **Limite d'arrêt de charge personnalisé de la batterie principale** : définissez le pourcentage de charge de la batterie qui doit être atteint avant que le terminal arrête de charger la batterie.
- **Peak Shift** : sélectionnez **Activer** pour utiliser le changement de crête afin de contrôler le moment où le terminal utilise sa batterie ou l'alimentation secteur. La fonctionnalité Peak Shift vous permet d'utiliser l'alimentation par batterie au lieu du courant alternatif pendant des périodes définies. Pour planifier la fonctionnalité **Peak Shift**, sélectionnez l'icône de calendrier.
- **Planification de la fonctionnalité Peak Shift** : les trois paramètres de la planification de la fonctionnalité Peak Shift permettent de contrôler les périodes durant lesquelles un terminal utilise sa batterie ou l'alimentation secteur et les périodes durant lesquelles il charge sa batterie.
  - **Démarrage de Peak Shift** : définissez l'heure à laquelle les terminaux doivent commencer à utiliser leurs batteries.
  - **Arrêt de Peak Shift** : définissez l'heure à laquelle les terminaux doivent utiliser l'alimentation CA.
  - **Démarrage de la charge Peak Shift** : définissez l'heure à laquelle les terminaux doivent commencer à charger leurs batteries en utilisant l'alimentation CA.
- **Seuil de la fonction Peak Shift de la batterie** : définissez le pourcentage de charge de la batterie qui doit être atteint avant que les terminaux cessent d'utiliser leurs batteries et passent à l'alimentation CA. Le paramètre **Démarrage de la charge Peak Shift** contrôle la période pendant laquelle les terminaux chargent leurs batteries après être passés à l'alimentation CA.

- **Propriétés système** : sélectionnez **Ajouter des propriétés système** pour ajouter une propriété système personnalisée. Cliquez à nouveau sur le bouton pour ajouter des propriétés supplémentaires. Ces propriétés correspondent à des options avancées. Pensez à consulter la documentation Dell avant d'utiliser ces paramètres. Les propriétés système remplacent tous les paramètres prédéfinis configurés dans le profil.
- **Classe** : entrez une classe et sélectionnez-la dans le menu déroulant. S'affiche après avoir sélectionné **Ajouter des propriétés système**.
- **Propriété système** : entrez une propriété système et sélectionnez-la dans le menu déroulant. S'affiche après avoir sélectionné **Ajouter des propriétés système**.
- **Attributs du BIOS** : sélectionnez **Ajouter un attribut du BIOS** pour ajouter un attribut du BIOS personnalisé. Cliquez à nouveau sur le bouton pour ajouter des attributs supplémentaires. Ces attributs correspondent à des options avancées. Pensez à consulter la documentation Dell avant d'utiliser ces paramètres. Les attributs du BIOS remplacent tous les paramètres prédéfinis configurés dans le profil.
- **Attribut du BIOS** : entrez un attribut du BIOS et sélectionnez-le dans le menu déroulant. S'affiche après avoir sélectionné **Ajouter un attribut du BIOS**.
- **Valeur** : sélectionnez une valeur pour l'attribut du BIOS. Si une valeur n'est pas fournie, l'attribut du BIOS est en lecture seule. S'affiche après avoir sélectionné **Ajouter un attribut du BIOS**.
- **Module de configuration** : sélectionnez **Importer** pour ajouter un module de configuration Dell Command | Configure. Importez un package vous permet de configurer plusieurs terminaux Dell avec une configuration unique. Les packages de configuration remplacent l'ensemble des propriétés ou attributs système personnalisés. Si vous approuvez les extensions de fichier autorisées, vous devez ajouter l'extension de fichier CCTK à la liste autorisée. Accédez à **Groupes et paramètres** > **Tous les paramètres** > **Contenu** > **Avancé** > **Extensions de fichiers** pour ajouter l'extension de fichier.

3. Cliquez sur **Enregistrer et publier**.

Profil Identifiants

Un profil Identifiants vous permet de déployer des certificats racine, intermédiaire et client sur les terminaux Windows afin de prendre en charge tous les cas d'utilisation d'infrastructure à clé publique (PKI) et d'authentification des certificats. Le profil déploie les identifiants configurés dans la zone de stockage adéquate sur le terminal Windows Desktop. Apprenez à configurer un profil Identifiants pour activer l'authentification pour vos terminaux Windows.

Même avec des mots de passe forts et d'autres restrictions, votre infrastructure reste vulnérable aux attaques par force brute, aux attaques de dictionnaire et aux erreurs des employés. Pour une sécurité renforcée, vous pouvez mettre en place des certificats numériques qui protégeront vos actifs professionnels. Pour utiliser les certificats de cette manière, vous devez d'abord configurer section de configuration Identifiants avec une autorité de certification, mais aussi vos propres sections de configuration Wi-Fi et VPN. Chacune de ces sections de configuration dispose de paramètres permettant d'associer l'autorité de certification définie dans la section de configuration

Identifiants.

Le profil Identifiants vous permet également d'envoyer des certificats S/MIME aux terminaux. Ces certificats sont chargés dans chaque compte d'utilisateur et sont contrôlés par le profil Identifiants.

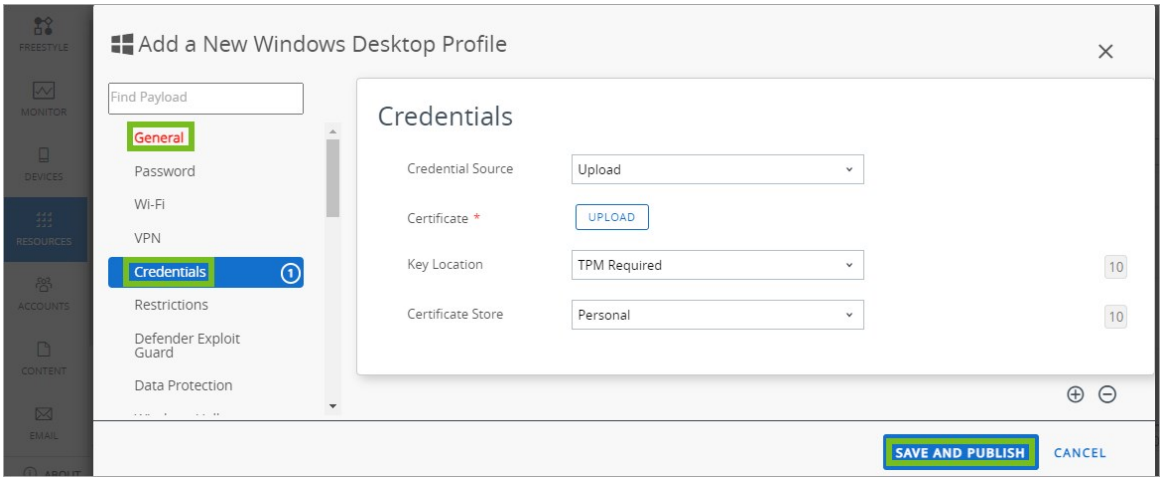
Configuration d'un profil Identifiants

Un profil Identifiants envoie des certificats aux terminaux pour qu'ils soient utilisés dans l'authentification. Avec Workspace ONE UEM, vous pouvez configurer les identifiants pour des magasins de certificat personnels, intermédiaires, de racines de confiance, de serveurs de publication approuvés et de personnes autorisées. Apprenez à configurer un profil Identifiants pour activer l'authentification pour vos terminaux Windows.

Même avec des mots de passe forts et d'autres restrictions, votre infrastructure reste vulnérable aux attaques par force brute, aux attaques de dictionnaire et aux erreurs des employés. Pour une sécurité renforcée, vous pouvez mettre en place des certificats numériques qui protégeront vos actifs professionnels. Pour utiliser les certificats de cette manière, vous devez d'abord configurer la charge utile des identifiants avec une autorité de certificat, mais aussi vos propres charges utiles Wi-Fi et VPN. Chacune de ces charges utiles dispose de paramètres permettant d'associer l'autorité de certificat définie dans la charge utile des identifiants.

Le profil Identifiants vous permet également d'envoyer en Push des certificats S/MIME aux terminaux. Ces certificats sont chargés dans chaque compte d'utilisateur et sont contrôlés par le profil Identifiants.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil d'utilisateur** ou **Profil du terminal**.
4. Configurez les **paramètres généraux** du profil.



5. Sélectionnez la section de configuration **Identifiants** et configurez les paramètres suivants :

Paramètres	Descriptions

Source des identifiants	Sélectionnez la source des identifiants **Importer**, **Autorité de certificat définie** ou **Certificat utilisateur**. Les options de section de configuration restantes dépendent de la source. Si vous sélectionnez Charger, vous devez charger un nouveau certificat. Si vous sélectionnez Autorité de certification définie, vous devez choisir une autorité de certification prédéfinie, ainsi qu'un modèle de certificat. Si vous sélectionnez Certificat utilisateur, vous devez sélectionner le mode d'utilisation du certificat S/MIME.
Importer	Sélectionnez ce paramètre pour naviguer vers le fichier de certificat d'identifiant requis et l'importer dans Workspace ONE UEM Console. Ce paramètre apparaît lorsque **Importer** est sélectionné en tant que **Source des identifiants**.
Autorité de certification	Utilisez le menu déroulant pour sélectionner une autorité de certification prédéfinie. Ce paramètre apparaît lorsque **Autorité de certification définie** est sélectionnée en tant que **Source des identifiants**.
Modèle de certificat	Utilisez le menu déroulant pour sélectionner un modèle de certificat prédéfini pour l'autorité de certification sélectionnée. Ce paramètre apparaît lorsque **Autorité de certification définie** est sélectionnée en tant que **Source des identifiants**.
Emplacement de la clé	Sélectionnez l'emplacement de la clé privée du certificat : **TPM si disponible** – Sélectionnez ce paramètre pour stocker la clé privée sur un Module de plateforme sécurisée (TPM) s'il y en a sur le terminal ; dans le cas contraire, stockez-la dans le système d'exploitation. **TPM obligatoire** – Sélectionnez ce paramètre pour stocker la clé privée sur un Module de plateforme sécurisée (TPM). S'il n'y a pas de TPM, le certificat ne peut pas être installé et une erreur s'affiche sur le terminal. **Logiciel** – Sélectionnez ce paramètre pour stocker la clé privée dans le système d'exploitation du terminal. **Passport** – Sélectionnez ce paramètre pour sauvegarder la clé privée dans Microsoft Passport. Cette option nécessite l'intégration d'Azure AD.
Magasin de certificats	Sélectionnez le magasin de certificats approprié pour que l'identifiant réside dans le terminal : **Personnel** – Sélectionnez ce paramètre pour stocker des certificats personnels. Les certificats personnels nécessitent la présence de Workspace ONE Intelligent Hub sur le terminal ou l'utilisation de la section SCEP. **Intermédiaire** – Sélectionnez ce paramètre pour stocker les certificats issus d'autorités de certification intermédiaires. **Racine de confiance** – Sélectionnez ce paramètre pour stocker des certificats provenant d'autorités de certification de confiance, ainsi que des certificats racines issus de votre organisation et de Microsoft. **Serveur de publication fiable** – Sélectionnez ce paramètre pour stocker des certificats provenant d'autorités de certification de confiance approuvées par des politiques de restriction de logiciels. **Personnes fiables** – Sélectionnez ce paramètre pour stocker des certificats provenant de personnes fiables ou d'entités explicitement approuvées. Il s'agit pour la plupart de certificats auto-signés ou de certificats explicitement approuvés dans une application telle que Microsoft Outlook.

Paramètres	Descriptions
Emplacement du magasin	Sélectionnez **Utilisateur** ou **Ordinateur** pour définir l'emplacement du certificat.
S/MIME	Indiquez si le certificat S/MIME est destiné au chiffrement ou à la signature. Cette option s'affiche uniquement si l'option **Source des informations d'identification** est définie sur **Certificat utilisateur**.

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

Profil des paramètres personnalisés

La section de configuration Paramètres personnalisés permet d'utiliser les fonctionnalités Windows Desktop que Workspace ONE UEM ne prend pas en charge actuellement par ses sections de configuration natives. Si vous souhaitez utiliser les nouvelles fonctionnalités, vous pouvez utiliser la charge utile des **Paramètres personnalisés** et le code XML pour activer ou désactiver certains paramètres manuellement.

Conditions prérequises

Pour un profil Windows Desktop, vous devez écrire votre propre code SyncML. Microsoft publie un site de référence Fournisseur de services de configuration disponible sur leur site Web. Pour créer un SyncML personnalisé, essayez le fling Créateur de stratégies disponible via le programme Flings VMware.

Exemple de code

```
  <Replace>
    <CmdID>2</CmdID>
      <Item>
        <Target>
          <LocURI>./Device/Vendor/MSFT/AssignedAccess/KioskModeApp</LocURI>
        </Target>
        <Meta>
          <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>{"Account":"standard","AUMID":"AirWatchLLC.AirWatchBrowser_htcwkw4rx2gx4
!App"}</Data>
      </Item>
  </Replace>
```

Procédure

1. Accédez au programme Flings VMware.
2. Sélectionnez la stratégie des fournisseurs de services de configuration que vous souhaitez utiliser pour créer votre profil personnalisé.
3. Cliquez sur **Configurer**.
4. Sur la page Configurer, configurez les paramètres de la stratégie pour répondre aux besoins de votre entreprise.

5. Sélectionnez la commande à utiliser avec la stratégie : **Ajouter**, **Supprimer**, **Enlever** ou **Remplacer**.
6. Sélectionnez le bouton **Copier**.
7. Dans Workspace ONE UEM Console, accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**, puis sélectionnez **Ajouter un profil**.
8. Sélectionnez **Windows**, puis **Windows Desktop**.
9. Sélectionnez **Profil d'utilisateur** ou **Profil du terminal**.
10. Configurez les **paramètres généraux** du profil.
11. Sélectionnez la section de configuration **Paramètres personnalisés** puis cliquez sur **Configurer**.
12. Sélectionnez une **Cible** pour le profil personnalisé.

    La plupart des cas d'utilisation utilisent **OMA-DM** comme **Cible**. Utilisez **Workspace ONE Intelligent Hub** lorsque vous personnalisez un profil BitLocker ou que vous cherchez à empêcher les utilisateurs de désactiver le service AirWatch.
13. Sélectionnez **Rendre les commandes atomiques** pour autant que votre SyncML utilise les commandes `Add`, `Delete` ou `Replace`. Si votre code utilise `Exec`, ne sélectionnez pas **Rendre les commandes atomiques**.
14. Collez le code XML que vous venez de copier dans la zone de texte **Paramètres d'installation**. Le code XML que vous collez doit contenir le bloc de code complet, qui va de `<Add>` à `</Add>` (ou similairement pour toute autre commande utilisée par votre code SyncML). N'incluez rien avant ou après ces balises.
15. Ajoutez le code de suppression à la zone de texte Supprimer des paramètres. Le code de suppression doit contenir les balises `<replace> </replace>` ou `<delete> </delete>`.

    Ce code permet l'exécution de fonctionnalités Workspace ONE UEM telles que Supprimer le profil et Désactiver le profil. Sans le code de suppression, vous ne pouvez pas supprimer le profil des terminaux sans transférer un deuxième profil Paramètres personnalisés. Pour plus d'informations, reportez-vous à l'article https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference.
16. Sélectionnez **Enregistrer et publier**.

Protection contre la désactivation par les utilisateurs du service Workspace ONE UEM

Utilisez un profil de paramètres personnalisés pour empêcher les utilisateurs finaux de désactiver Workspace ONE UEM (AirWatch) Service sur leurs terminaux Windows. Empêcher les utilisateurs finaux de désactiver le service Workspace ONE UEM garantit que Workspace ONE Intelligent Hub exécute des check-ins réguliers avec Workspace ONE UEM Console et reçoit les dernières mises à jour de la stratégie.

1. Créez un profil **Paramètres personnalisés**.
2. Définissez la **Cible** sur **Agent de protection**.
3. Copiez le code suivant et collez-le dans la zone de texte **Paramètres personnalisés**.

```
          <wap-provisioningdoc id="c14e8e45-792c-4ec3-88e1-be121d8c33dc" name="
customprofile">
            <characteristic type="com.airwatch.winrt.awservicelockdown" uuid="7
957d046-7765-4422-9e39-6fd5eef38174">
              <parm name="LockDownAwService" value="True"/>
            </characteristic>
          </wap-provisioningdoc>
```

4. Cliquez sur **Enregistrer et publier**. Si vous souhaitez supprimer la restriction pour les terminaux de l'utilisateur, vous devez envoyer un profil distinct en utilisant le code suivant.

```
          <wap-provisioningdoc id="c14e8e45-792c-4ec3-88e1-be121d8c33dc" name="
customprofile">
            <characteristic type="com.airwatch.winrt.awservicelockdown" uuid="7
957d046-7765-4422-9e39-6fd5eef38174">
              <parm name="LockDownAwService" value="False"/>
            </characteristic>
          </wap-provisioningdoc>
```

Profil Dynamic Environment Manager (DEM)

VMware Dynamic Environment Manager (DEM) fournit une expérience utilisateur persistante pour les sessions utilisateur sur les terminaux Windows. Les fonctionnalités incluent la personnalisation des paramètres de Windows et d'application, ainsi que l'exécution d'actions de l'utilisateur et de l'ordinateur pour certains déclencheurs ou lors du lancement d'applications. Vous pouvez intégrer Dynamic Environment Manager et Workspace ONE UEM pour utiliser ces fonctionnalités avec le profil DEM.

Le profil DEM dans Workspace ONE UEM déploie un profil de configuration DEM créé dans la console de gestion VMware Dynamic Environment Manager (console de gestion DEM). Le profil de configuration DEM fonctionne sur les terminaux Windows gérés par Workspace ONE UEM, qu'ils soient virtuels, physiques ou basés sur le Cloud. Sur le terminal, Workspace ONE Intelligent Hub pour Windows et DEM FlexEngine extraient et appliquent vos profils.

Documentation DEM

Pour plus d'informations sur VMware Dynamic Environment Manager, reportez-vous au site VMware Docs.

CDN requis

Le CDN est requis pour cette fonctionnalité.

- Si vous disposez d'un environnement SaaS et que vous avez désactivé CDN, vous devez l'activer, sinon l'intégration DEM ne sera pas disponible.
- Si vous disposez d'un environnement sur site et que vous n'utilisez pas ou n'avez pas configuré CDN, l'intégration DEM n'est pas disponible.

Critères à prendre en compte

- Dans DEM, utilisez le mode **UEM intégré** pour créer le profil de configuration DEM. Si vous n'utilisez pas ce mode, vous ne pouvez pas créer de profils de configuration DEM. Workspace ONE UEM ne prend actuellement pas en charge SMB pour la configuration DEM.
- Assurez-vous que vos configurations dans Dynamic Environment Manager et Workspace ONE UEM ne sont pas en conflit. Par exemple, ne restreignez pas certaines configurations dans une console et ne les autorisez pas dans une autre.
- Dans Workspace ONE UEM, n'attribuez pas plusieurs profils DEM à un seul terminal. L'attribution de plusieurs profils DEM à un seul terminal peut entraîner le déploiement de configurations incorrectes.
- Extrayez et installez la console de gestion DEM et DEM FlexEngine à l'aide du processus d'installation **personnalisé** et non le processus d'installation par défaut. Le processus d'installation par défaut installe uniquement la console de gestion DEM.
- Utilisez DEM v2106 ou version ultérieure, car cette intégration n'est pas prise en charge dans les versions antérieures.

Tâches à effectuer avant l'intégration

Avant de pouvoir intégrer VMware Dynamic Environment Manager (DEM) et Workspace ONE UEM, vous devez installer la console de gestion DEM et déployer DEM FlexEngine sur des terminaux gérés.

- Téléchargez et extrayez la console de gestion DEM et de DEM FlexEngine.
    - Accédez au site VMware Customer Connect pour VMware Dynamic Environment Manager.
    - Téléchargez les versions applicables de la console et du moteur.
- Installez la console de gestion DEM sur un terminal sur lequel vous souhaitez créer des profils de configuration.
    - Basculez la console de gestion DEM vers le mode **UEM intégré** en choisissant `Configure | Integration | Workspace ONE UEM Integration`.
- Lorsque vous créez votre profil de configuration DEM, effectuez les tâches suivantes comme indiqué dans Installation de FlexEngine en mode NoAD.
    - Incluez un fichier NoAD.xml dans le cadre de votre configuration.
    - Incluez un fichier de licence en en important un à partir de l'icône du menu principal dans la console de gestion DEM.
    - Enregistrez le profil de configuration DEM afin de pouvoir le télécharger vers Workspace ONE UEM à l'aide du profil DEM.
- Déployez DEM FlexEngine en tant qu'application (MSI) sur des terminaux gérés Windows avec Workspace ONE UEM. Les terminaux gérés nécessitent à la fois l'interface DEM FlexEngine et Workspace ONE Intelligent Hub pour Windows afin d'appliquer les profils de configuration DEM sur le terminal.
    1. Dans Workspace ONE UEM Console, sélectionnez le groupe organisationnel applicable.

2. Accédez à **Ressources > Applications > Natives > Internes**.
3. Téléchargez le fichier MSI DEM FlexEngine.
4. Dans l'onglet **Options de déploiement**, activez le mode **UEM intégré** sur la ligne de commande pendant l'installation.
    1. Accédez à la section **Comment installer**.
    2. Entrez la commande dans la zone de texte **Installer la commande**. Exemple : `msiexec.exe /i "VMware Dynamic Environment Manager Enterprise 2106 10.3 x64.msi" /qn INTEGRATION_ENABLED=1`
5. **Enregistrez et attribuez** l'application pour la déployer dans les Smart Groups appropriés qui incluent vos terminaux gérés Windows.

Configuration d'un profil DEM

Utilisez les profils de terminaux Workspace ONE UEM pour déployer vos configurations DEM (Dynamic Environment Manager) sur vos terminaux Windows gérés.

1. Dans Workspace ONE UEM Console, accédez à **Ressources > Profils et lignes de base > Profils > Ajouter**, puis sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis choisissez **Windows Desktop** en tant que plateforme.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil. La section de configuration **Général** inclut l'attribution des Smart Groups. Attribuez les Smart Groups qui incluent vos terminaux gérés Windows pour qu'ils reçoivent le profil de configuration DEM.
5. Sélectionnez la charge utile **Dynamic Environment Manager** (DEM).
6. Utilisez la page **DEM** pour télécharger le fichier de configuration DEM et sélectionnez **Enregistrer et publier** pour terminer les configurations.

Workspace ONE UEM déploie le profil de configuration DEM sur les terminaux gérés dans les Smart Groups attribués. Le DEM FlexEngine et Workspace ONE Intelligent Hub pour Windows appliquent vos profils de configuration DEM. Les modifications de profil ne sont visibles qu'après la fermeture et l'ouverture de session sur le terminal une fois le déploiement du profil effectué par le système.

Application des modifications du profil de configuration DEM

L'utilisateur du terminal doit fermer sa session, puis se reconnecter au terminal géré Windows afin de voir les modifications de profil déployées par les profils de configuration DEM.

Profil Protection des données

Le profil Protection des données configure des règles pour contrôler la manière dont les applications d'entreprise ont accès aux données de différentes sources de votre organisation. Découvrez comment l'utilisation du profil de protection des données garantit que vos données ne sont accessibles que par des applications sécurisées et approuvées.

Lorsque les données personnelles et d'entreprise se trouvent sur un même terminal, elles peuvent être divulguées par accident à des services que votre organisation ne contrôle pas. Grâce à la section de configuration Protection des données, Workspace ONE UEM contrôle le mouvement des

données d'entreprise entre les applications afin de limiter les fuites et de réduire l'impact sur les utilisateurs. Workspace ONE UEM utilise la fonctionnalité WIP (Windows Information Protection) de Microsoft pour protéger vos terminaux Windows.

La protection des données approuve les applications d'entreprise, ce qui leur accorde l'accès aux données de l'entreprise issues de réseaux protégés. Si un utilisateur déplace des données vers des applications qui n'appartiennent pas à l'entreprise, vous pouvez agir en fonction des politiques de mise en application sélectionnées.

La fonctionnalité WIP traite les données comme étant des données d'entreprise non chiffrées ou comme des données personnelles à protéger et à chiffrer. Les applications approuvées pour la protection des données se répartissent en quatre types. Ces types déterminent le mode d'interaction de l'application avec les données protégées.

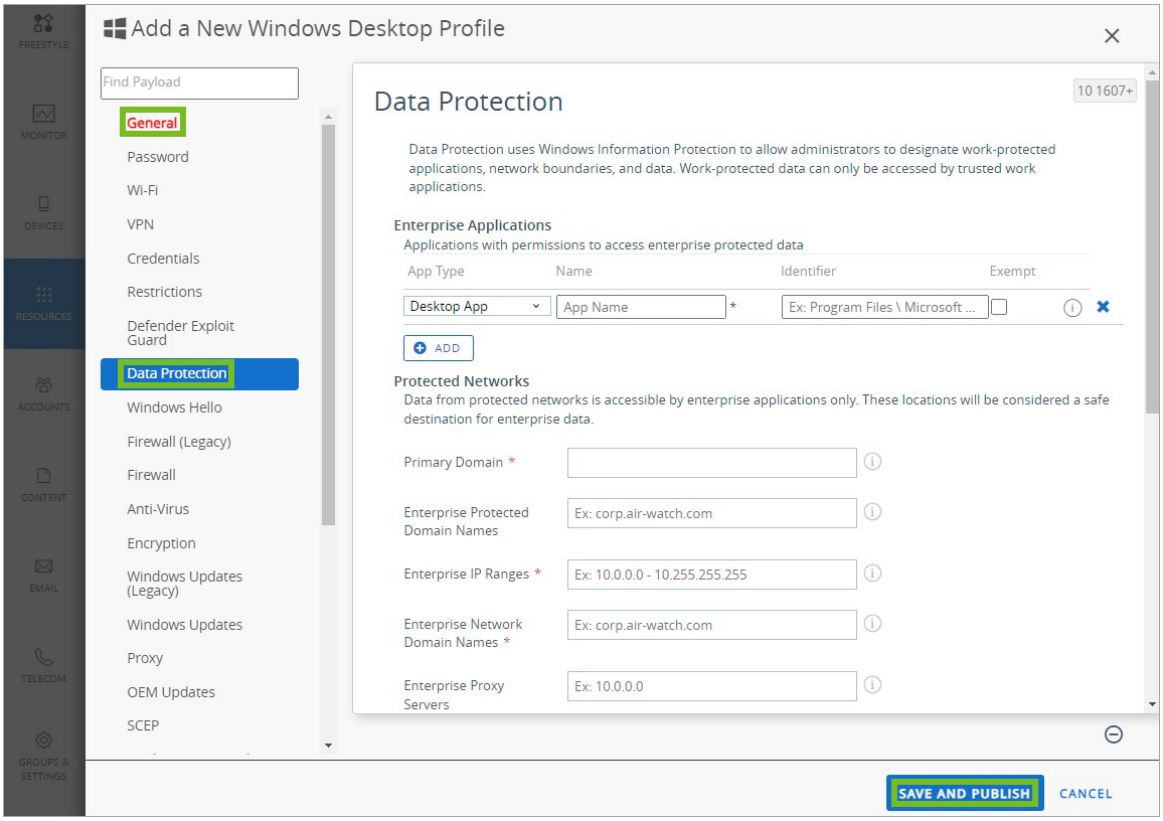
- Applications renseignées – Ces applications prennent entièrement en charge la fonctionnalité WIP. Les applications renseignées peuvent accéder sans problèmes aux données personnelles et aux données d'entreprise. Si les données sont créées avec une application renseignée, vous pouvez les enregistrer en tant que données personnelles non chiffrées ou en tant que données d'entreprise chiffrées. Vous pouvez empêcher les utilisateurs d'enregistrer leurs données personnelles avec des applications renseignées à l'aide du profil Protection des données.
- Applications autorisées – Ces applications prennent en charge les données chiffrées par la fonctionnalité WIP. Les applications autorisées ont accès aux données personnelles et d'entreprise, mais elles enregistrent toutes les données auxquelles elles accèdent en tant que données d'entreprise chiffrées. Elles enregistrent les données personnelles en tant que données d'entreprise chiffrées qui ne sont pas accessibles à l'extérieur des applications approuvées par la fonctionnalité WIP. Il est conseillé d'approuver au cas par cas les applications afin d'éviter tout problème d'accès aux données. Pour plus d'informations sur l'approbation de la fonctionnalité WIP, consultez les fournisseurs de logiciel.
- Applications exemptées – Vous déterminez les applications exemptées de mise en application de la politique WIP lorsque vous créez le profil Protection des données. Exemptez toutes les applications qui ne prennent pas en charge les données chiffrées par la fonctionnalité WIP. Si une application ne prend pas en charge le chiffrement WIP, elle se bloque si elle essaie d'accéder à des données d'entreprise chiffrées. Aucune politique WIP ne s'applique qu'aux applications exemptées. Les applications exemptées ont accès aux données personnelles non chiffrées et aux données d'entreprise chiffrées. Étant donné qu'elles ont accès aux données d'entreprise sans mise en application d'une politique WIP, procédez avec prudence lorsque vous approuvez des applications exemptées. Les applications exemptées créent des écarts dans la protection de données et la fuite des données d'entreprise.
- Applications non autorisées – Ces applications ne sont pas approuvées, ne sont pas exemptées des politiques WIP et n'ont pas accès aux données d'entreprise chiffrées. Les applications non autorisées ont toujours accès aux données personnelles qui se trouvent sur un terminal protégé par la fonctionnalité WIP.

Important : le profil Protection des données nécessite la protection WIP (Windows Information Protection). Cette fonctionnalité nécessite la mise à jour anniversaire de Windows. Vous pouvez tester ce profil avant de le déployer en production.

Configuration d'un profil Protection des données

Créez le profil Protection des données (aperçu) pour utiliser la fonctionnalité Protection des informations Microsoft Windows afin de limiter l'accès des utilisateurs et des applications aux données de votre organisation dans des applications et des réseaux approuvés. Vous pouvez définir les contrôles détaillés de la protection des données.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis choisissez **Windows Desktop** en tant que plateforme.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez la charge utile **Protection des données**.



6. Configurez les paramètres Protection des données d'entreprise :

Paramètres	Descriptions
Ajout	Sélectionnez ce paramètre pour ajouter des applications d'entreprise à la liste des entreprises autorisées. Les applications ajoutées ici sont fiables et autorisées à utiliser des données d'entreprise.
Type d'application	Déterminez si cette application est une application de bureau standard ou une application du Microsoft Store. Vous pouvez également sélectionner un éditeur d'applications ou stocker des applications. Le fait de sélectionner un éditeur approuve toutes les applications de cet éditeur.

Paramètres	Descriptions
Nom	Saisissez le nom de l'application. Si l'application est une application Microsoft Store, sélectionnez l'icône **Recherche** pour rechercher le nom de la famille de modules (PFN) de l'application.
Identifiant	Indiquez le chemin d'accès au fichier d'une application de bureau ou le nom de la famille de packages dans le cas d'une application de magasin.
Exempté	Cochez cette case si l'application ne prend pas en charge la protection complète des données, mais a encore besoin d'accéder aux données d'entreprise. L'activation de cette option exempte l'application de toute restriction en matière de protection des données. Ces applications sont souvent des applications existantes qui ne prennent pas encore en charge la protection des données. La création d'exemptions crée des écarts dans la protection des données. Créez des exemptions uniquement lorsque c'est nécessaire.
Domaine principal	Saisissez le domaine principal qu'utilisent vos données d'entreprise. Les données provenant de réseaux protégés sont accessibles par les applications d'entreprise uniquement. Une tentative d'accès à un réseau protégé émanant d'une application qui ne figure pas sur la liste des applications autorisées de l'entreprise entraînera la mise en application d'une politique. Saisissez le nom des domaines en minuscules uniquement.
Noms de domaines protégés d'entreprise	Entrez la liste des domaines (autres que le domaine principal) utilisée par l'entreprise pour ses identités utilisateur. Séparez les domaines par une barre verticale `|`. Saisissez le nom des domaines en minuscules uniquement.
Plages d'adresses IP d'entreprise	Saisissez les plages d'adresses IP d'entreprise qui définissent les terminaux Windows dans le réseau d'entreprise. Les données issues des terminaux figurant dans cette plage sont considérées comme faisant partie de l'entreprise et sont protégées. Ces emplacements sont considérés comme étant des destinations sûres pour le partage des données d'entreprise.
Noms de domaines de réseaux d'entreprise	Saisissez la liste des domaines qui définissent les limites du réseau d'entreprise. Les données d'un domaine répertorié qui est envoyé à un terminal sont considérées comme étant des données d'entreprise et sont protégées. Ces emplacements sont considérés comme étant des destinations sûres pour le partage des données d'entreprise.
Serveurs proxy d'entreprise	Saisissez la liste des serveurs proxy que l'entreprise peut utiliser pour les ressources d'entreprise.
Ressources d'entreprise dans le Cloud	Saisissez la liste des domaines de ressources d'entreprise hébergés dans le Cloud et qui doivent être protégés par routage par l'intermédiaire du réseau et d'un serveur proxy (port 80). Si Windows ne peut pas déterminer si une application peut être autorisée à se connecter à une ressource réseau, il bloque automatiquement la connexion. Si vous souhaitez que, par défaut, Windows autorise les connexions, ajoutez la chaîne `/*AppCompat*/` au paramètre. Par exemple : `www.air-watch.com | /*AppCompat*/` Ajoutez la chaîne `/*AppCompat*/` uniquement pour changer le paramètre par défaut.

Paramètres	Descriptions
Niveau de protection des données d'application	Définissez le niveau de protection et les actions à entreprendre pour protéger les données d'entreprise.
Afficher les icônes EDP	Activez ce paramètre pour afficher une icône EDP dans le navigateur Web, l'explorateur de fichiers et les icônes d'application lors de l'accès aux données protégées. L'icône s'affiche également dans les vignettes d'application professionnelle du menu Démarrer.
Révoquer après un désenrôlement	Activez ce paramètre pour révoquer les clés de protection des données d'un terminal lorsque ce dernier est désenrôlé de Workspace ONE UEM.
Déchiffrement utilisateur	Activez ce paramètre pour autoriser les utilisateurs à sélectionner le mode d'enregistrement des données à l'aide d'une application compatible. Ils peuvent sélectionner Enregistrer comme données d'entreprise ou Enregistrer comme données personnelles. Si cette option n'est pas activée, toutes les données enregistrées à l'aide d'une application compatible sont enregistrées en tant que données d'entreprise et sont chiffrées à l'aide du système de chiffrement de l'entreprise.
Accès direct à la mémoire	Activez ce paramètre pour autoriser des utilisateurs à accéder directement à la mémoire du terminal.
Certificat de récupération des données	Importez le certificat spécial intitulé « Système de fichiers EFS » utilisé pour la récupération de fichiers, dans le cas où votre clé de chiffrement serait perdue ou endommagée.

7. Cliquez sur **Enregistrer et publier** pour envoyer le profil vers les terminaux.

Création d'un certificat de système de fichiers chiffré

Le profil Protection des données chiffre les données d'entreprise et limite l'accès aux terminaux approuvés. Créez un certificat EFS pour chiffrer les données de votre entreprise par un profil Protection des données.

1. Sur un ordinateur sans certificat EFS, ouvrez une invite de commande (avec droits administrateur) et accédez au magasin de certificats dans lequel vous souhaitez stocker le certificat.
2. Exécutez la commande : `cipher /r:<EFSRA>`

   Valeur deest le nom des fichiers.cer et.pfx que vous souhaitez créer.
3. Lorsque vous y êtes invité, saisissez le mot de passe afin de protéger votre nouveau fichier .pfx.
4. Les fichiers .cer et .pfx sont créés dans le magasin de certificats que vous avez sélectionné.
5. Importez votre certificat .cer dans les terminaux dans le cadre d'un profil Protection des données.

Profil Defender Exploit Guard

Protégez vos terminaux Windows des failles d'exploitation et des logiciels malveillants avec le profil Windows Defender Exploit Guard. Workspace ONE UEM utilise ces paramètres pour protéger vos terminaux des failles d'exploitation, réduire les surfaces d'attaque, contrôler l'accès aux dossiers et protéger vos connexions réseau.

Windows Defender Exploit Guard

Divers programmes malveillants et failles d'exploitation utilisent les vulnérabilités de vos terminaux Windows pour accéder à votre réseau et à vos terminaux. Workspace ONE UEM utilise le profil Windows Defender Exploit Guard pour protéger vos terminaux de ces acteurs malintentionnés. Le profil utilise les paramètres Windows Defender Exploit Guard natifs de Windows. Le profil contient quatre méthodes de protection différentes. Ces méthodes couvrent différentes vulnérabilités et vecteurs d'attaque.

Exploit Protection

Exploit Protection applique automatiquement des atténuations de failles d'exploitation au système d'exploitation et aux applications. Ces atténuations fonctionnent également avec les antivirus tiers et Windows Defender. Dans le profil de Windows Defender Exploit Guard, vous configurez ces paramètres en téléchargeant un fichier XML de configuration. Ce fichier doit être créé à l'aide de l'application de sécurité Windows ou de PowerShell.

Réduction de la surface d'attaque

Les règles de réduction de la surface d'attaque permettent d'éviter les actions typiques que les logiciels malveillants utilisent pour infecter des terminaux. Ces règles visent des actions telles que :

- Fichiers exécutables et scripts utilisés dans les applications Office ou la messagerie Web qui essaient de télécharger ou d'exécuter des fichiers
- Scripts obfusqués ou suspects
- Actions non généralement utilisées par les applications

Les règles de réduction de la surface d'attaque requièrent que la protection en temps réel de Windows Defender soit activée.

Accès contrôlé aux dossiers

L'accès contrôlé aux dossiers permet de protéger vos données précieuses contre les applications et les menaces malveillantes, y compris les ransomware. Lorsque ce paramètre est activé, l'antivirus Windows Defender passe en revue toutes les applications (.EXE, .SCR, .DLL, etc.).
Windows Defender détermine ensuite si l'application est malveillante ou sûre. Si l'application est marquée comme malveillante ou suspecte, Windows empêche l'application de modifier les fichiers dans les dossiers protégés.

Les dossiers protégés incluent des dossiers système communs. Vous pouvez ajouter des dossiers à la fonctionnalité Accès contrôlé aux dossiers. La plupart des applications connues et approuvées peuvent accéder aux dossiers protégés. Si vous souhaitez qu'une application interne ou inconnue accède à des dossiers protégés, vous devez ajouter le chemin d'accès au fichier d'application lors de

la création du profil.

L'accès contrôlé aux dossiers requiert que la protection en temps réel de Windows Defender soit activée.

Protection réseau

La protection réseau permet de protéger les utilisateurs et les données contre les tentatives d'hameçonnage et les sites Web malveillants. Ces paramètres empêchent les utilisateurs d'utiliser n'importe quelle application pour accéder à des domaines dangereux pouvant héberger des attaques par hameçonnage, des exploits ou des logiciels malveillants.

La protection réseau requiert que la protection en temps réel de Windows Defender soit activée.

Informations supplémentaires

Pour plus d'informations sur les paramètres configurés et les protections contre les exploits spécifiques, reportez-vous à https://docs.microsoft.com/en-us/sccm/protect/deploy-use/create-deploy-exploit-guard-policy.

Création d'un profil Defender Exploit Guard

Créez un profil Defender Exploit Guard avec Workspace ONE UEM pour protéger vos terminaux Windows contre les failles et les logiciels malveillants. Découvrez comment utiliser le profil pour configurer les paramètres de Windows Defender Exploit Guard sur vos terminaux Windows.

Lorsque vous créez des règles et des paramètres pour **Réduction de la surface d'attaque**, **Accès contrôlé aux dossiers** et **Protection réseau**, vous devez sélectionner Activé, Désactivé ou Audit. Ces options modifient le fonctionnement de la règle ou du paramètre.

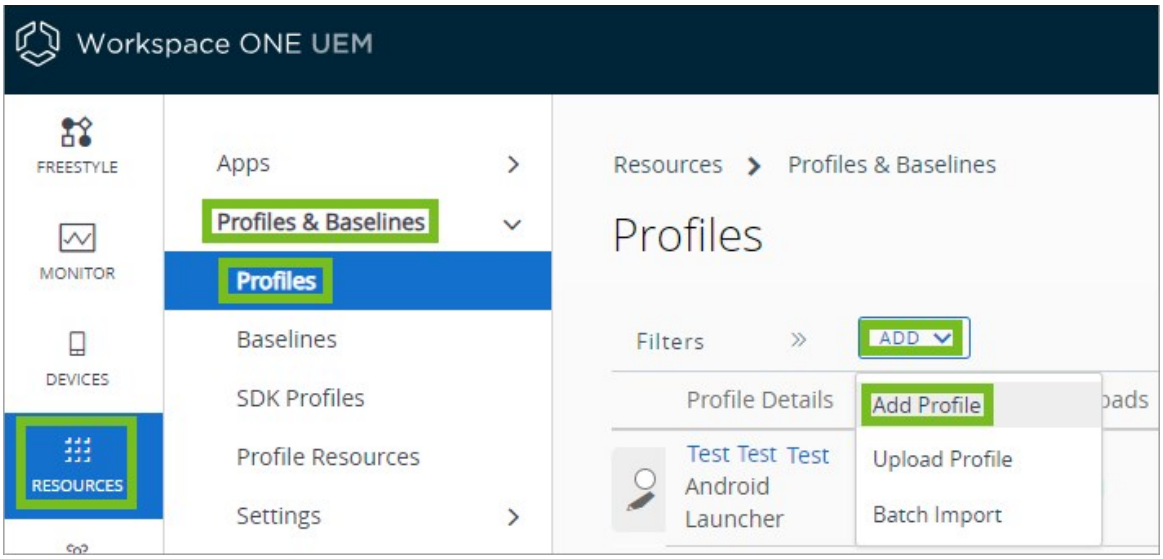
- Activé : configure Windows Defender pour bloquer les failles d'exploitation pour cette méthode. Par exemple, si vous définissez l'option Accès contrôlé aux dossiers sur Activé, Windows Defender empêchera les failles d'exploitations d'accéder aux dossiers protégés.
- Désactivé : ne configure pas la stratégie pour Windows Defender.
- Audit : configure Windows Defender pour bloquer les failles d'exploitation de la même manière que l'option Activé, mais consigne également l'événement dans l'observateur d'événements.

Conditions prérequises

Pour utiliser les paramètres Exploit Protection sur ce profil, vous devez créer un fichier XML de configuration à l'aide de l'application de sécurité Windows ou de PowerShell sur un terminal individuel avant de créer le profil.

Procédure

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



2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez la section de configuration **Defender Exploit Guard**.
6. Téléchargez le fichier XML de configuration **Paramètres Exploit Protection**.

   Ces paramètres appliquent automatiquement des techniques d'atténuation des exploits au système d'exploitation et aux applications individuelles. Vous devez créer le fichier XML à l'aide de l'application de sécurité Windows ou de PowerShell sur un terminal individuel.
7. Configurez les paramètres de **Réduction de la surface d'attaque**. Ces règles permettent d'éviter les actions typiques que les programmes malveillants utilisent pour infecter des terminaux avec du code malveillant. Sélectionnez **Ajouter** pour ajouter des règles supplémentaires.

   La description de chaque règle définit les applications ou les types de fichiers auxquels la règle s'applique. Les règles de réduction de la surface d'attaque requièrent que la protection en temps réel de Windows Defender soit activée.
8. Configurez les paramètres d'**Accès contrôlé aux dossiers**. Définissez **Accès contrôlé aux dossiers** sur **Activé** pour utiliser ces paramètres. Lorsqu'il est activé, ce paramètre protège plusieurs dossiers par défaut. Pour afficher la liste, passez votre curseur sur l'icône **?** Ces paramètres protègent automatiquement vos données contre les programmes malveillants et les failles d'exploitation. L'accès contrôlé aux dossiers requiert que la protection en temps réel de Windows Defender soit activée.
   - Ajoutez des dossiers supplémentaires à protéger en sélectionnant **Ajouter** et saisissez le chemin d'accès au fichier de dossiers.
   - Ajoutez des applications pouvant accéder aux dossiers protégés en sélectionnant **Ajouter** et en saisissant le chemin d'accès au fichier d'application. La plupart des applications connues et approuvées peuvent accéder aux dossiers par défaut. Utilisez ce paramètre pour ajouter des applications internes ou inconnues pouvant accéder aux dossiers protégés.

9. Configurez les paramètres de Protection réseau. Définissez **Protection réseau** sur **Activée** pour utiliser ces paramètres. Ces paramètres protègent les utilisateurs et les données contre les tentatives d'hameçonnage et les sites Web malveillants. La protection réseau requiert que la protection en temps réel de Windows Defender soit activée.
10. Sélectionnez **Enregistrer et publier** lorsque vous avez terminé pour envoyer le profil sur les terminaux.

Profil Chiffrement

Sécurisez les données de votre organisation sur les terminaux Windows Desktop à l'aide du profil Chiffrement. Le profil Chiffrement définit la stratégie de chiffrement BitLocker sur vos terminaux Windows Desktop afin d'assurer la sécurité des données.

Le chiffrement BitLocker est uniquement disponible sur les terminaux Windows Entreprise, Éducation et Pro.

Par leur conception, les ordinateurs portables et les tablettes sont des terminaux mobiles : les données de votre entreprise risquent d'être perdues ou dérobées. En mettant en application une politique de chiffrement via Workspace ONE UEM, vous pouvez protéger vos données sur disque dur. BitLocker est la méthode de chiffrement Windows native et Dell Data Protection | Encryption est une solution de chiffrement tierce de Dell. Si le profil Chiffrement est activé, Workspace ONE Intelligent Hub vérifie en permanence l'état de chiffrement du terminal. Si Workspace ONE Intelligent Hub s'aperçoit que le terminal n'est pas chiffré, il le chiffre automatiquement.

Si vous décidez de chiffrer avec BitLocker, une clé de récupération créée lors du chiffrement est stockée pour chaque lecteur (s'il est configuré) dans Workspace ONE UEM Console. L'administrateur a la possibilité de faire des clés de récupération une clé à usage unique. Si cette option est sélectionnée, une nouvelle clé de récupération est générée après son utilisation. L'utilisateur devra ensuite contacter l'administrateur pour obtenir la nouvelle clé de récupération mise à jour. Pour plus d'informations, reportez-vous à la section Clés de récupération.

Le profil Chiffrement nécessite l'installation de Workspace ONE Intelligent Hub sur le terminal.

Remarque : Le profil Chiffrement ne peut en outre ni configurer ni activer Dell Data Protection | Encryption. L'état du chiffrement est remonté dans Workspace ONE UEM Console et dans le portail self-service, mais le chiffrement doit être configuré manuellement sur le terminal.

Attention : Windows ne prend pas en charge les terminaux sans clavier virtuel dans l'écran de préinitialisation. Sans clavier, vous ne pouvez pas entrer le code PIN d'initialisation nécessaire au déverrouillage du disque dur et au démarrage de Windows sur le terminal. L'envoi de ce profil à des terminaux sans clavier dans l'écran de préinitialisation bloque votre terminal.

Fonctionnalité BitLocker

Le profil Chiffrement utilise la fonctionnalité BitLocker afin de contrôler l'authentification et le déploiement du chiffrement BitLocker.

BitLocker utilise le module de plateforme sécurisée (TPM) sur les terminaux pour stocker la clé de chiffrement du terminal. Si le lecteur est retiré de la carte mère, il reste chiffré. Pour une authentification améliorée, vous pouvez activer un code PIN de chiffrement afin de démarrer le système. Vous pouvez également exiger un mot de passe pour les terminaux lorsqu'un TPM n'est

pas disponible.

Comportement du déploiement

Le chiffrement BitLocker natif Windows permet de sécuriser les données sur les terminaux Windows Desktop. Le déploiement du profil de chiffrement peut nécessiter des actions supplémentaires de la part de l'utilisateur final, telles que la création d'un code PIN ou d'un mot de passe.

Si le profil Chiffrement est envoyé à un terminal chiffré et que les paramètres de chiffrement correspondent à ceux du profil, Workspace ONE Intelligent Hub ajoute une protection BitLocker et envoie une clé de récupération à Workspace ONE UEM Console.

Avec cette fonctionnalité, si un utilisateur ou un administrateur tente de désactiver BitLocker sur le terminal, le profil Chiffrement peut le chiffrer à nouveau. Le chiffrement est appliqué même si le terminal est hors ligne.

Si le chiffrement en vigueur ne correspond pas aux paramètres d'authentification du profil Chiffrement, les protecteurs existants sont supprimés et de nouveaux protecteurs sont appliqués conformément aux paramètres du profil Chiffrement.

Si la méthode de chiffrement existante ne correspond pas au profil Chiffrement, Workspace ONE UEM la conserve. Cette fonctionnalité s'applique également lorsque vous ajoutez une version du profil Chiffrement à un terminal géré par un profil Chiffrement existant. La méthode de chiffrement existante est conservée.

Remarque : Les modifications du profil BIOS s'appliquent après les profils de chiffrement. Les modifications apportées au profil BIOS, telles que la désactivation ou l'effacement du TPM, peuvent provoquer un événement de récupération qui requiert la clé de récupération pour redémarrer le système. Interrompez BitLocker avant d'apporter des modifications au BIOS.

États de chiffrement

Si BitLocker est activé et en cours d'utilisation, vous pouvez voir des informations sur l'état du chiffrement dans les zones répertoriées.

- **Détails du terminal** Workspace ONE UEM
    - Les détails du terminal affichent des informations sur la clé de récupération. Utilisez le lien **Afficher la clé de récupération** pour afficher et copier les clés de récupération de tous les lecteurs chiffrés.
    - Vous trouverez plusieurs états BitLocker dans l'onglet **Résumé**, **Chiffré**, **Chiffrement en cours**, **Déchiffrement en cours**, **Interrompu** et **Partiellement protégé**.
        - L'état **Interrompu (X redémarrages restants)** reflète l'interruption de la protection du disque, bien que le disque soit toujours chiffré. Vous pouvez voir cet état si un système d'exploitation est en cours de mise à jour ou si des modifications sont en cours au niveau du système. Une fois que le nombre de redémarrages est épuisé, la protection par BitLocker est automatiquement réactivée.
        - Le statut **Partiellement protégé** reflète la situation dans laquelle le lecteur du système d'exploitation est chiffré, mais pas les autres.
    - Dans l'onglet **Sécurité** des **Détails du terminal**, affichez l'état de chiffrement et la

méthode de chiffrement de vos lecteurs. Vous pouvez savoir en un coup d'œil si une machine n'utilise pas le niveau de chiffrement que vous avez défini dans le profil de chiffrement. Workspace ONE UEM affiche uniquement la méthode de chiffrement. Il ne déchiffre pas les disques, même s'ils ne correspondent pas au paramètre **Méthode de chiffrement** du profil **Chiffrement**.

- Portail self-service Workspace ONE UEM
  - La page Sécurité du Portail en libre-service affiche la clé de récupération BitLocker.
  - La protection BitLocker apparaît comme activée.

Clés de récupération

Workspace ONE UEM dépose des clés de récupération pour le **Lecteur de l'OS et Tous les disques durs fixes** lorsque ce paramètre est activé pour **Volume chiffré** dans le profil **Chiffrement**. Si un lecteur doit être récupéré, la clé de récupération est disponible pour chacun des lecteurs.

L'administrateur a la possibilité de rendre les clés de récupération à usage unique en sélectionnant **Activer une clé de récupération à usage unique** dans les paramètres **Profil de chiffrement**. Pour plus d'informations, reportez-vous à la section Configuration d'un profil de chiffrement. Si cette option est activée, une fois qu'une clé de récupération est utilisée pour récupérer un lecteur, une nouvelle clé de récupération est générée par Intelligent Hub et est redéposée dans UEM Console.

Pendant une courte période, jusqu'à ce que la nouvelle clé de récupération soit correctement déposée dans UEM Console, la clé de récupération personnelle précédente (ancienne) et la clé de récupération personnelle (nouvelle) sont toutes les deux disponibles. En cas de dépôt réussi de la nouvelle clé de récupération, la clé de récupération précédente sera supprimée et ne pourra plus être utilisée pour la récupération du lecteur.

Vous pouvez voir, à des fins de dépannage, quel utilisateur a récupéré un lecteur externe avec une clé spécifique, quand une récupération a eu lieu et quel administrateur a contribué au processus. Dans Workspace ONE UEM Console, accédez à **Terminaux > Affichage des détails > Plus - Dépannage > Journal des événements** pour trouver les détails.

Comportement de suppression

Si le profil est supprimé de Workspace ONE UEM Console, Workspace ONE UEM n'applique plus le chiffrement et le terminal est automatiquement déchiffré. Le nettoyage par l'entreprise ou la désinstallation manuelle de Workspace ONE Intelligent Hub à partir du Panneau de configuration désactive le chiffrement BitLocker.

Lorsque vous créez le profil de chiffrement, vous pouvez activer l'option **Toujours maintenir le système chiffré**. Ce paramètre garantit que le terminal reste chiffré même si le profil est supprimé, si le contenu du terminal est effacé ou si la communication avec Workspace ONE UEM se termine.

Si l'utilisateur décide de désenrôler le terminal durant le processus de chiffrement BitLocker, ce processus continue jusqu'à ce qu'il soit désactivé manuellement dans le Panneau de configuration.

BitLocker et stratégies de conformité

Vous pouvez configurer des stratégies de conformité pour prendre en charge l'état de chiffrement BitLocker que vous souhaitez appliquer. Dans la section Règles d'une stratégie de conformité, sélectionnez **Chiffrement** > **Est**, puis **Non appliqué au lecteur système**, **Non appliqué à certains**

lecteurs (partiellement protégé) ou **Interrompu**.

Prise en charge de BitLocker To Go

Grâce au profil de chiffrement, vous pouvez imposer le chiffrement de lecteurs externes sur vos terminaux Windows à l'aide de BitLocker. Cochez **Activer la prise en charge de BitLocker To Go** pour activer cette fonctionnalité. Les lecteurs externes restent en lecture seule jusqu'à ce qu'ils soient chiffrés. En sélectionnant une option dans le menu déroulant Méthode de chiffrement, vous pouvez choisir la méthode à utiliser pour chiffrer le terminal.

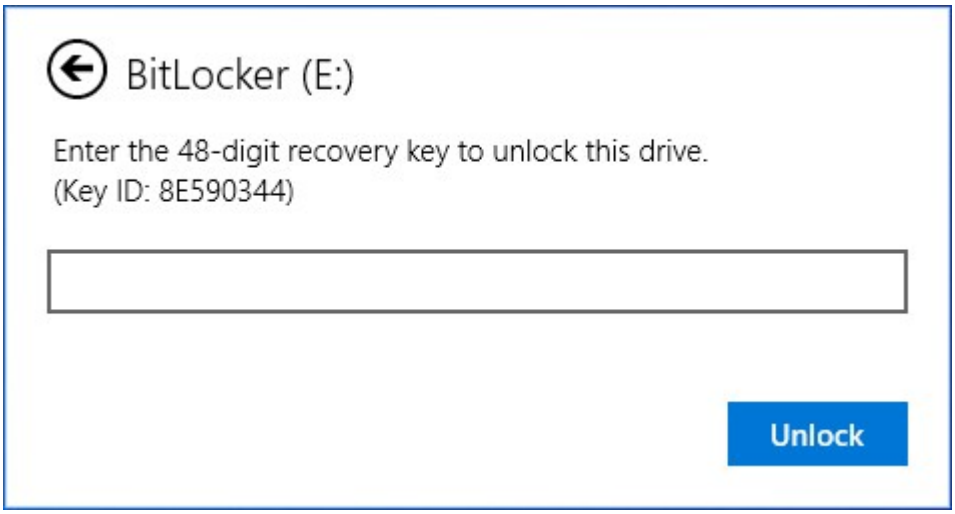
Workspace ONE Intelligent Hub pour Windows demande à vos utilisateurs de créer un mot de passe pour accéder aux lecteurs et les utiliser. La longueur minimale de ce mot de passe peut être définie par l'administrateur dans la console sous **Paramètres BitLocker To Go**. Une fois que les utilisateurs ont branché le lecteur chiffré sur le terminal Windows, ils doivent utiliser leur mot de passe pour accéder au lecteur, copier du contenu sur le lecteur, modifier des fichiers, supprimer du contenu ou effectuer toute autre tâche impliquant un lecteur externe. L'administrateur peut également choisir s'il souhaite chiffrer uniquement l'espace utilisé sur le lecteur ou l'ensemble du lecteur.

Où trouver les informations de la clé de récupération ?

Si les utilisateurs oublient leur mot de passe, vous pouvez récupérer les lecteurs depuis la console dans **Terminaux > Périphériques > Affichage en liste > Stockage externe**. Utilisez le lien **Vue** pour que le lecteur copie la clé de récupération et l'envoie à l'utilisateur concerné par e-mail. Vous pouvez également accéder à cette page depuis le compte de l'utilisateur dans **Comptes > Utilisateurs > Affichage en liste**. Sélectionnez l'utilisateur concerné et allez dans l'onglet **Stockage externe**.

Pour les déploiements qui comprennent des milliers d'ID de récupération, vous pouvez filtrer le contenu sur la page **Stockage externe**. Il y a plusieurs façons de filtrer le contenu.

- Assurez-vous que l'utilisateur vous fournisse l'**ID de clé**, sélectionnez le curseur de filtre dans la colonne **ID de récupération** puis entrez la valeur. L'ID de récupération avec cet ID de clé s'affiche dans les résultats.



- Sélectionnez le curseur de filtre dans la colonne **Nom d'utilisateur** et entrez le nom d'utilisateur concerné pour trouver le lecteur et sa clé de récupération.

Vous pouvez voir, à des fins d'audit, quel utilisateur a récupéré un lecteur externe avec une clé spécifique, quand une récupération a eu lieu et quel administrateur a contribué au processus. Dans

la console Workspace ONE UEM, allez dans **Terminaux > Périphériques > Affichage en liste > Événements** pour plus de détails.

Vous pouvez consulter les informations de clé pour chaque utilisateur. Dans la console Workspace ONE UEM, allez dans **Comptes > Utilisateurs > Affichage en liste**, puis sélectionnez l'utilisateur. Si l'utilisateur a chiffré au moins un lecteur, un onglet **Stockage externe** sera disponible dans son historique.

Interrompre BitLocker dans la console

Vous pouvez désormais interrompre et reprendre le chiffrement BitLocker depuis la console. Cet élément de menu est ajouté en tant qu'action dans les enregistrements des terminaux. Vous le trouverez dans **Terminaux > Affichage en liste**. Sélectionnez le terminal puis l'élément de menu **Plus d'actions**. Cette option est particulièrement utile pour les utilisateurs qui ont besoin d'aide avec leur terminal mais qui n'ont pas les autorisations nécessaires pour gérer BitLocker.

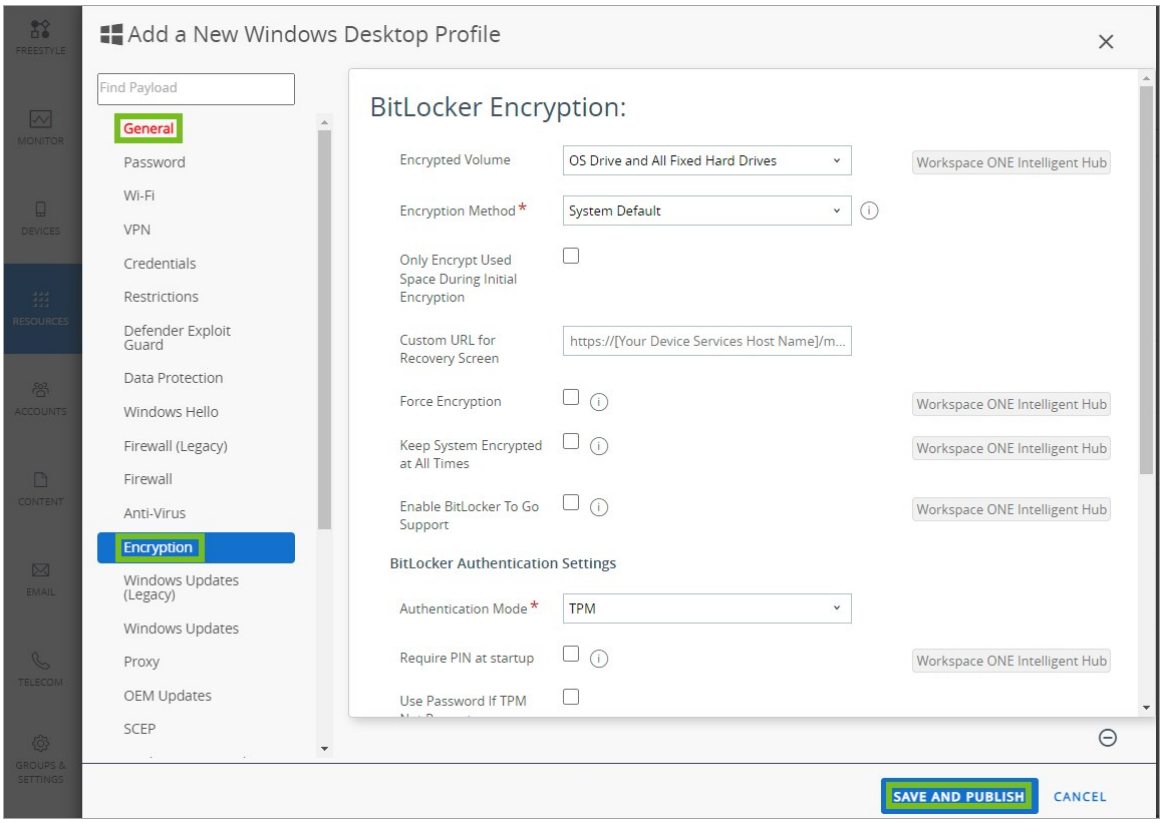
Quand vous choisissez d'**Interrompre BitLocker** pour un terminal, la console affiche plusieurs options, dont notamment **Nombre de redémarrages**. Par exemple, pour aider un utilisateur à mettre à jour son BIOS, le système peut avoir besoin de redémarrer deux fois, auquel cas sélectionnez **3**. Cette valeur permet au système de redémarrer une fois de plus avec un chiffrement interrompu, de sorte que le BIOS se met à jour correctement avant la reprise BitLocker.

Si toutefois vous ignorez combien de redémarrages seront nécessaires à une tâche, sélectionnez une valeur plus élevée. Une fois la tâche terminée, vous pouvez utiliser l'option **Plus d'actions > Reprendre BitLocker**.

Configurer un profil Chiffrement

Créez un profil **Chiffrement** pour sécuriser vos données sur les terminaux Windows Desktop à l'aide des chiffrements BitLocker natif et BitLocker To Go.

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.



5. Sélectionnez le profil **Chiffrement** et configurez les paramètres.

Paramètres	Descriptions
Volume chiffré	Utilisez le menu déroulant pour sélectionner le type de chiffrement comme suit : **Lecteur de l'OS et Tous les disques durs fixes** : chiffre tous les disques durs sur le terminal, y compris la partition système sur laquelle est installé le système. **Lecteur de l'OS** – Chiffre le lecteur sur lequel Windows est installé et à partir duquel il démarre.
Méthode de chiffrement	Sélectionnez la méthode de chiffrement du terminal.
Méthode de chiffrement de la valeur système par défaut	Cochez cette case si votre OEM spécifie une méthode de chiffrement par défaut pour un type de terminal donné. Ce paramètre applique l'algorithme de chiffrement par défaut.
Chiffrer uniquement l'espace utilisé lors du chiffrement initial	Activez ce paramètre pour limiter le chiffrement BitLocker à l'espace utilisé sur le lecteur au moment du chiffrement.
URL personnalisée pour la clé de récupération	Saisissez l'URL à afficher sur l'écran de verrouillage afin de diriger les utilisateurs vers le lieu d'obtention de la clé de récupération. Pensez à saisir l'URL du portail self-service, étant donné que Workspace ONE UEM y héberge la clé de récupération.

Paramètres	Descriptions
Forcer le chiffrement	Activez ce paramètre pour forcer le chiffrement sur le terminal. Cela signifie que le terminal est immédiatement de nouveau chiffré si BitLocker est désactivé manuellement. Pensez à désactiver ce paramètre pour éviter des problèmes pendant les mises à niveau ou les effacements des données professionnelles.
Maintenir le système chiffré à tout moment	Activez cette option pour que le terminal soit toujours chiffré. Utilisez cette option pour vous assurer que les effacements du contenu du terminal, les suppressions des profils ou les interruptions de communication avec Workspace ONE UEM ne déchiffrent pas le terminal. Si vous activez ce paramètre et effacez le contenu d'un terminal, vous pouvez uniquement accéder à la récupération sur Workspace ONE UEM Console pendant 30 jours. Après 30 jours, le système peut être irrécupérable.
Activer la prise en charge de BitLocker To Go	Activez cette option pour exiger de BitLocker qu'il chiffre les lecteurs amovibles sur les terminaux Windows. Lorsque cette option est sélectionnée, les lecteurs externes restent en lecture seule jusqu'à ce qu'ils soient chiffrés. L'administrateur peut configurer la méthode de chiffrement, la longueur minimale du mot de passe et s'il souhaite chiffrer uniquement l'espace utilisé l'ensemble du lecteur lors du chiffrement initial. Les utilisateurs doivent créer un mot de passe pour accéder aux lecteurs. Si vos utilisateurs oublient leur mot de passe, recherchez les ID de récupération et les clés de ces lecteurs chiffrés dans la console depuis **Terminaux > Périphériques > Affichage en liste > Stockage externe**.
Paramètres d'authentification BitLocker : Mode d'authentification	Sélectionnez la méthode pour authentifier l'accès à un terminal chiffré par BitLocker. **TPM** — Utilise le module de plateforme sécurisée (TPM). Requiert un TPM sur le terminal. **Mot de passe** — Utilise un mot de passe pour l'authentification.
Paramètres d'authentification BitLocker : Exiger un code PIN au démarrage	Sélectionnez la case à cocher pour exiger des utilisateurs qu'ils saisissent un code PIN pour démarrer le terminal. Cette option empêche le démarrage de l'OS et la reprise automatique depuis le mode de suspension ou d'hibernation jusqu'à ce que les utilisateurs entrent le code approprié.
Paramètres d'authentification BitLocker : Longueur du code PIN	Sélectionnez ce paramètre pour configurer une longueur spécifique de code PIN au démarrage. Ce code PIN est numérique, sauf s'il est configuré avec **Autoriser le code PIN amélioré** au démarrage.
Paramètres d'authentification BitLocker : Autoriser le code PIN amélioré au démarrage	Cochez cette case pour permettre aux utilisateurs de définir des codes PIN avec autre chose que des chiffres. Les utilisateurs peuvent définir des majuscules et des minuscules, utiliser des symboles, des chiffres et des espaces. Si la machine ne prend pas en charge les codes PIN améliorés dans un environnement de prédémarrage, ces paramètres ne fonctionnent pas.

Paramètres	Descriptions
Paramètres d'authentification BitLocker : Utiliser le mot de passe si TPM n'est pas présent	Sélectionnez cette case à cocher pour utiliser un mot de passe comme solution de secours afin de chiffrer le terminal si TPM n'était pas disponible. Si ce paramètre n’est pas activé, tous les terminaux ne disposant pas de puce TPM ne seront pas chiffrés.
Paramètres d'authentification BitLocker : Interrompre BitLocker jusqu'à l'initialisation du TPM	Sélectionnez cette option pour reporter le chiffrement sur le terminal jusqu'à ce que le TPM soit initialisé sur la machine. Utilisez cette option pour les enrôlements qui nécessitent un chiffrement avant que le TPM ne s'initialise, comme OOBE.
Paramètres d'authentification BitLocker : Longueur minimale du mot de passe	Sélectionnez le nombre minimum de caractères requis pour le mot de passe. Cette option s'affiche si le **Mode d'authentification** est défini sur **Mot de passe** ou si **Utiliser le mot de passe en cas d'absence du TPM**est activé.

| Paramètres de la clé de récupération BitLocker : Activer la clé de récupération à usage unique | Cochez la case pour rendre les clés de récupération à usage unique. Une fois que la clé est utilisée, une nouvelle clé de récupération est générée. L'utilisateur doit contacter l'administrateur pour obtenir la clé de récupération mise à jour.|

| Paramètres de la clé de récupération BitLocker statique : Créer une clé BitLocker statique | Cochez la case si une clé de récupération statique est activée. | | Paramètres de la clé de récupération BitLocker statique : Mot de passe de récupération BitLocker | Sélectionnez l'icône **Générer** afin de générer une nouvelle clé de récupération. | | Paramètres de la clé de récupération BitLocker statique : Période de rotation | Saisissez le nombre de jours jusqu'à la rotation de la clé de récupération. | | Paramètres de la clé de récupération BitLocker statique : Période de grâce | Saisissez le nombre de jours après la rotation pendant lesquels la clé de récupération précédente fonctionne toujours. | | Interrompre BitLocker : Activer la suspension de BitLocker | Cochez la case pour activer la suspension de BitLocker. Cette fonctionnalité permet d'interrompre le chiffrement BitLocker pendant une durée spécifique.

Utilisez cette fonction pour interrompre BitLocker lorsque des mises à jour sont planifiées, de sorte que les terminaux puissent redémarrer sans que l'utilisateur ne doive saisir un code PIN ou un mot de passe de chiffrement. | | Interrompre BitLocker : Type de suspension de BitLocker | Sélectionnez le type de suspension.

Planification — Sélectionnez cette option pour saisir une durée spécifique d'interruption du BitLocker. Définissez ensuite la répétition planifiée sur Quotidienne ou Hebdomadaire.
Personnalisée — Sélectionnez cette option pour saisir la date et l'heure de début et de fin de l'interruption de BitLocker. | | Interrompre BitLocker : Heure de début de la suspension de BitLocker | Entrez l'heure de début de la suspension de BitLocker. | | Interrompre BitLocker : Heure de fin de la suspension de BitLocker | Entrez l'heure de fin de la suspension de BitLocker. | | Interrompre

BitLocker : Type de répétition planifiée | Définissez si la suspension planifiée se répète tous les jours ou toutes les semaines. Si vous choisissez une répétition hebdomadaire, sélectionnez les jours de la semaine impliqués. |

1. Sélectionnez **Enregistrer et publier** lorsque vous avez terminé pour envoyer le profil sur les terminaux.

Profil Exchange ActiveSync

Les profils Exchange ActiveSync vous permettent de configurer les terminaux Windows Desktop afin qu'ils accèdent au serveur Exchange ActiveSync pour utiliser la messagerie et l'agenda.

Utilisez des certificats signés par une autorité de certification tierce approuvée (CA). Des erreurs dans les certificats exposent les connexions sécurisées autrement à d'éventuelles attaques de type MITM. De telles attaques dégradent la confidentialité et l'intégrité des données transmises entre composants de produit, et risquent même de donner aux attaquants la possibilité d'intercepter ou d'altérer les données en transit.

Le profil Exchange ActiveSync prend en charge le client de messagerie natif pour Windows Desktop. La configuration change en fonction du client de messagerie que vous utilisez.

Suppression de profils ou effacement des données d'entreprise

Si le profil est supprimé par une commande de suppression, des politiques de conformité ou un effacement des données d'entreprise, toutes les données de la messagerie sont effacées, notamment :

- Le compte utilisateur/les informations de connexion
- Les données des messages
- Les informations des contacts et de l'agenda
- Les pièces jointes enregistrées dans le stockage des applications internes

Nom d'utilisateur et mot de passe

Si les identifiants e-mail sont différents des adresses e-mail, vous pouvez utiliser le champ **{EmailUserName}**, qui correspond aux identifiants e-mail importés lors de l'intégration des services d'annuaire. Même si les noms d'utilisateur sont identiques aux adresses mail, utilisez la zone de texte **{EmailUserName}**, car elle utilise les adresses mail importées par l'intégration des services d'annuaire.

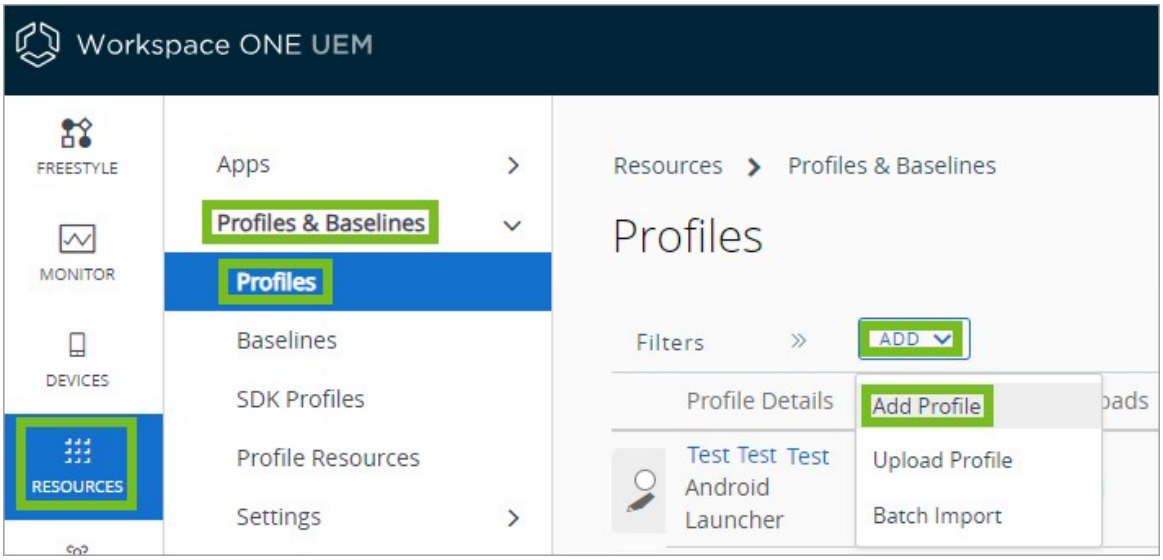
Créez un profil Exchange ActiveSync pour fournir aux terminaux Windows Desktop l'accès au serveur Exchange ActiveSync afin qu'ils utilisent la messagerie et l'agenda.

Configuration d'un profil Exchange ActiveSync

Créez un profil Exchange ActiveSync pour fournir aux terminaux Windows Desktop l'accès au serveur Exchange ActiveSync afin qu'ils utilisent la messagerie et l'agenda.

Remarque : Workspace ONE UEM ne prend pas en charge Outlook 2016 pour les profils Exchange ActiveSync. La configuration de profil Services Web Exchange (EWS) pour l'application Outlook sur un terminal Windows Desktop via Workspace ONE UEM n'est plus prise en charge dans la version 2016 de Microsoft Exchange.

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



2. Sélectionnez **Windows**, puis choisissez **Windows Desktop** en tant que plateforme.
3. Sélectionnez **Profil d'utilisateur**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez la section de configuration **Exchange ActiveSync**.
6. Configurez les paramètres Exchange ActiveSync :

Paramètres	Descriptions
Client de messagerie	Sélectionnez le client de messagerie que le profil EAS configure. Workspace ONE UEM prend en charge le client de messagerie natif.
Nom du compte	Saisissez le nom du compte Exchange ActiveSync.
Hôte Exchange ActiveSync	Saisissez l'URL ou l'adresse IP du serveur qui héberge le serveur EAS.
Utiliser le SSL	Envoyez toutes les communications par Secure Socket Layer.
Domaine	Saisissez le domaine de messagerie. Le profil prend en charge les valeurs de recherche pour y indiquer les informations de connexion de l'utilisateur de l'enrôlement.
Nom d'utilisateur	Saisissez le nom d'utilisateur de messagerie.
Adresse e-mail	Saisissez l'adresse e-mail. Cette zone de texte est un paramètre obligatoire.
Mot de passe	Saisissez le mot de passe de messagerie.
Certificat d'identité	Sélectionnez le certificat pour la section de configuration EAS.
Prochain intervalle de synchronisation (min)	Sélectionnez la fréquence, en minutes, à laquelle le terminal se synchronise avec le serveur EAS.
Synchronisation des e-mails depuis	Sélectionnez depuis combien de jours les e-mails se synchronisent avec le terminal.
Journalisation du diagnostic	Activez cette option afin de journaliser des informations pour des raisons de dépannage.

Paramètres	Descriptions
Exiger la protection des données lorsque le terminal est verrouillé	Activez cette option pour exiger que les données soient protégées lorsque le terminal est verrouillé.
Autoriser la synchronisation des e-mails	Activez cette option pour autoriser la synchronisation des e-mails.
Autoriser la synchronisation des contacts	Activez cette option pour autoriser la synchronisation des contacts.
Autoriser la synchronisation du calendrier	Activez cette option pour autoriser la synchronisation d'événements de calendrier.

7. Sélectionnez **Enregistrer** pour conserver le profil dans Workspace ONE UEM Console ou **Enregistrer et publier** pour envoyer le profil aux terminaux.

Profil Services Web Exchange

Créez un profil Services Web Exchange pour permettre aux utilisateurs d'accéder aux infrastructures de messagerie et aux comptes Microsoft Outlook de l'entreprise à partir de leurs terminaux.

Important : Au cours de la première configuration, le terminal doit avoir accès au serveur Exchange interne.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil d'utilisateur**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Services Web Exchange** et configurez les paramètres :

Paramètres	Descriptions
Domaine	Saisissez le nom du domaine de messagerie auquel appartient l'utilisateur.
Serveur de messagerie	Saisissez le nom du serveur Exchange.
Adresse e-mail	Saisissez l'adresse e-mail du compte de messagerie.

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

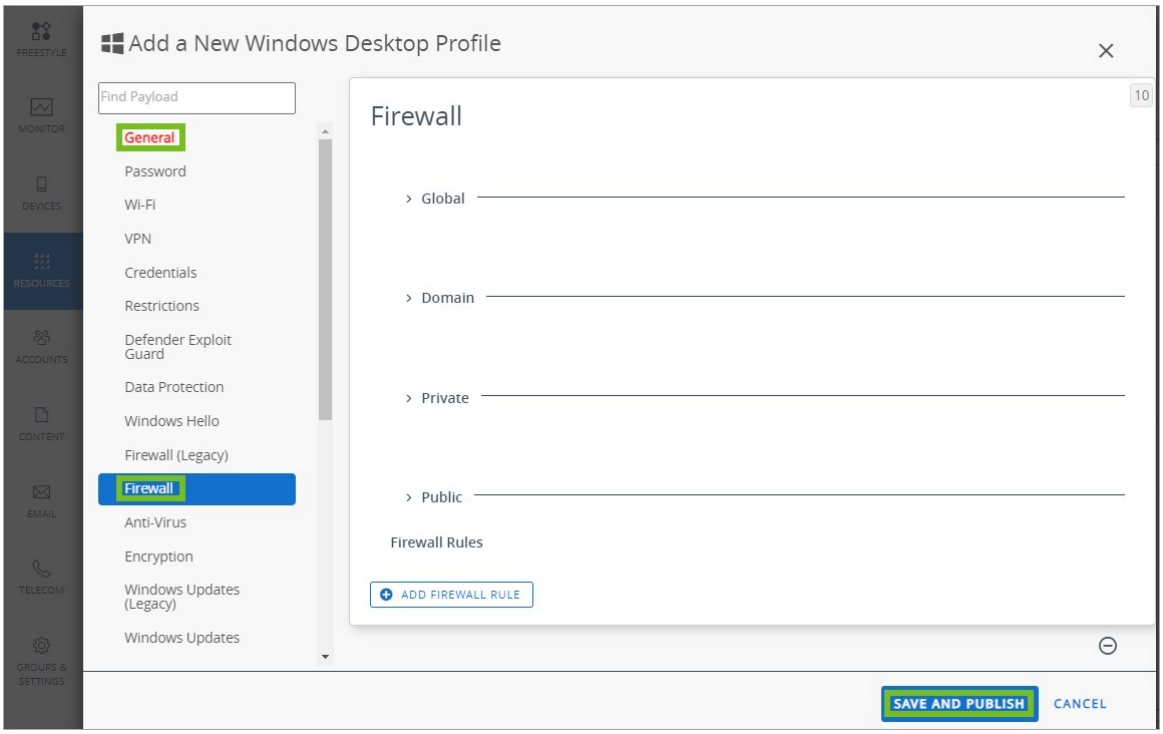
   La suppression d'un profil Services Web Exchange a pour effet de supprimer tous les comptes Outlook du terminal.

Profil Pare-feu

Créez un profil Pare-feu pour configurer les paramètres natifs du pare-feu Windows Desktop. Ce profil utilise des fonctionnalités plus avancées que le profil de pare-feu (Hérité).

Workspace ONE UEM approuve automatiquement l'agent OMA-DM pour vous assurer que Workspace ONE UEM Console peut toujours communiquer avec les terminaux.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.



5. Sélectionnez la section de configuration **Pare-feu**.
6. Configurez les paramètres **Globaux**.

Paramètre	Description
FTP avec état	Définissez la manière dont le pare-feu gère le trafic FTP. Si vous sélectionnez Activer, le pare-feu effectue le suivi de tout le trafic FTP. Si vous sélectionnez **Désactiver**, le pare-feu n'inspecte pas le trafic FTP.
Durée d'inactivité de l'association de sécurité	Sélectionnez **Configurer** et définissez la durée maximale (en secondes) pendant laquelle le terminal attend avant de supprimer les associations de sécurité inactives. Les associations de sécurité constituent un accord entre deux pairs ou points de terminaison. Ces accords contiennent toutes les informations requises pour échanger des données en toute sécurité.
Codage de la clé prépartagée	Sélectionnez le type de codage utilisé pour la clé prépartagée.
Exemptions IPSec	Sélectionnez les exemptions IPSec à utiliser.
Vérification de la liste de révocation des certificats	Sélectionnez le mode d'application de la vérification de la liste de révocation de certificat.

Paramètre	Description
Jeu d'authentification de correspondance d'opportunité par KM	Sélectionnez la manière dont les modules de clés ignorent les suites d'authentification. L'activation de cette option force les modules clés à ignorer uniquement les suites d'authentification qu'ils ne prennent pas en charge. La désactivation de cette option force les modules clés à ignorer la totalité de l'ensemble d'authentification s'ils ne prennent pas en charge toutes les suites d'authentification dans l'ensemble.
Activer la file d'attente de paquets	Sélectionnez la manière dont le mode paquet en file d'attente fonctionne sur le terminal. Ce paramètre vous permet de garantir une mise à l'échelle appropriée.

7. Configurez le comportement du pare-feu lorsqu'il est connecté aux réseaux **Domaine**, **Privé** et **Public**.

Paramètre	Description
Firewall	Définissez sur **Activer** pour appliquer les paramètres de la stratégie sur le trafic réseau. Si ce paramètre est désactivé, le terminal autorise tout le trafic réseau, quels que soient les autres paramètres de la stratégie.
Action sortante	Sélectionnez l'action par défaut que le pare-feu effectue sur les connexions sortantes. Si vous définissez ce paramètre sur **Bloquer**, le pare-feu bloque tout le trafic sortant, sauf spécification contraire explicite.
Action entrante.	Sélectionnez l'action par défaut que le pare-feu effectue sur les connexions entrantes. Si vous définissez ce paramètre sur **Bloquer**, le pare-feu bloque tout le trafic entrant, sauf spécification contraire explicite.
Réponses de type monodiffusion au trafic réseau de type diffusion ou multidiffusion	Définissez le comportement des réponses pour le trafic réseau de type multidiffusion ou diffusion. Si vous désactivez cette option, le pare-feu bloque toutes les réponses au trafic réseau de type multidiffusion ou diffusion.
Notifier l'utilisateur lorsque le pare-feu Windows bloque une nouvelle application	Définissez le comportement de notification du pare-feu. Si vous sélectionnez **Activer**, le pare-feu peut envoyer des notifications à l'utilisateur lorsqu'il bloque une nouvelle application. Si vous sélectionnez **Désactiver**, le pare-feu n'envoie aucune notification.
Mode furtif	Pour définir le terminal en mode furtif, sélectionnez **Activer**. Le mode furtif permet d'empêcher les acteurs malintentionnés d'obtenir des informations sur les terminaux et les services de réseau. Lorsque ce paramètre est activé, le mode furtif bloque les messages sortants ICMP inaccessibles et TCP de réinitialisation des ports sans que l'application écoute activement ce port.
Autoriser le trafic réseau IPSec en mode furtif	Définissez la manière dont le pare-feu gère le trafic non sollicité sécurisé par IPSec. Si vous sélectionnez **Activer**, le pare-feu autorise le trafic réseau non sollicité sécurisé par IPSec. Ce paramètre s'applique uniquement lorsque vous activez le Mode furtif.
Règles de pare-feu local	Définissez la manière dont le pare-feu interagit avec les règles de pare-feu local. Si vous sélectionnez **Activer**, le pare-feu suit les règles locales. Si vous sélectionnez Désactiver, le pare-feu ignore les règles locales et ne les applique pas.

Paramètre	Description
Règles de connexion locale	Définissez la manière dont le pare-feu interagit avec les règles locales de connexion de sécurité. Si vous sélectionnez **Activer**, le pare-feu suit les règles locales. Si vous sélectionnez Désactiver, le pare-feu ignore les règles locales et ne les applique pas, quelles que soient les versions de sécurité de schéma et de connexion.
Règles de pare-feu du port global	Définissez la manière dont le pare-feu interagit avec les règles de pare-feu du port global. Si vous sélectionnez **Activer**, le pare-feu suit les règles de pare-feu de port global. Si vous sélectionnez **Désactiver**, le pare-feu ignore les règles et ne les applique pas.
Règles d'application autorisées	Définissez la manière dont le pare-feu interagit avec les règles locales d'application autorisées. Si vous sélectionnez **Activer**, le pare-feu suit les règles locales. Si vous sélectionnez Désactiver, le pare-feu ignore les règles locales et ne les applique pas.

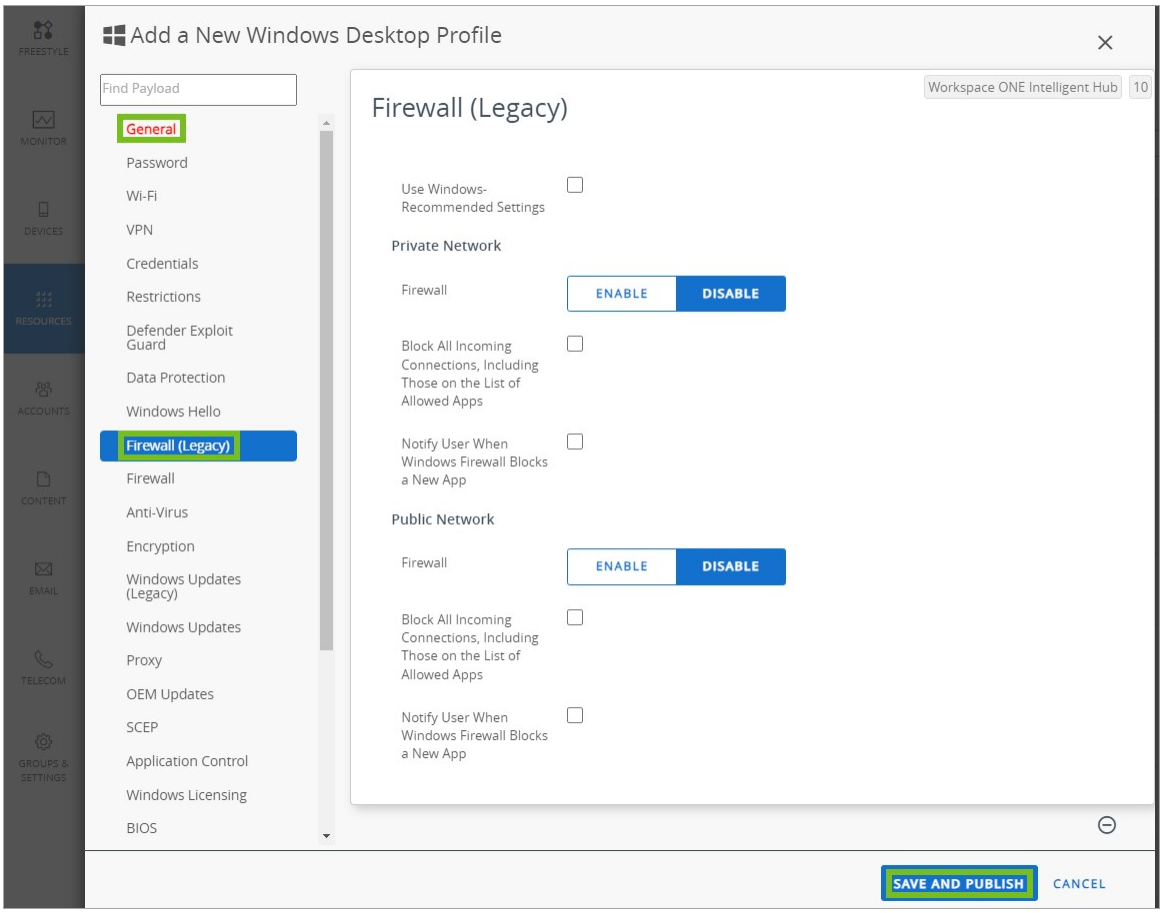
8. Pour configurer vos propres règles de pare-feu, sélectionnez **Ajouter une règle de pare-feu**. Après avoir ajouté une règle, configurez les paramètres selon vos besoins. Vous pouvez ajouter autant de règles que vous le voulez.
9. Une fois l'ajout terminé, cliquez sur **Enregistrer et publier** pour envoyer le profil vers les terminaux.

Profil Pare-feu (Hérité)

Le profil Pare-feu (Hérité) pour les terminaux Windows Desktop vous permet de configurer les paramètres de pare-feu Windows pour les terminaux. Envisagez d'utiliser le nouveau profil de pare-feu pour Windows Desktop, car le nouveau profil utilise les nouvelles fonctionnalités de Windows.

Important : Le profil Pare-feu nécessite l'installation de Workspace ONE Intelligent Hub sur le terminal.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.



5. Sélectionnez la section de configuration **Pare-feu (Hérité)**.
6. Activez **Utiliser les paramètres recommandés par Windows** pour utiliser les paramètres recommandés par Windows et désactivez toutes les autres options disponibles pour ce profil. Les paramètres seront automatiquement modifiés sur les paramètres recommandés et vous ne pourrez pas les modifier.
7. Configurez les paramètres de **Réseau privé** :

Paramètres	Description
Firewall	Activez cette fonctionnalité pour utiliser le pare-feu lorsque le terminal est connecté sur un réseau privé.
Bloquer toutes les connexions entrantes, y compris celles provenant de la liste des applications autorisées	Activez pour bloquer toutes les connexions entrantes. Ce paramètre autorise les connexions sortantes.
Notifier l'utilisateur lorsque le pare-feu Windows bloque une nouvelle application	Activez ce paramètre pour autoriser l'affichage de notifications lorsque le pare-feu Windows bloque une nouvelle application.

8. Configurez les paramètres de **Réseau public** :

Paramètres	Description
Firewall	Activez cette fonctionnalité pour utiliser le pare-feu lorsque le terminal est connecté sur un réseau privé.

Paramètres	Description
Bloquer toutes les connexions entrantes, y compris celles provenant de la liste des applications autorisées	Activez pour bloquer toutes les connexions entrantes. Ce paramètre autorise les connexions sortantes.
Notifier l'utilisateur lorsque le pare-feu Windows bloque une nouvelle application	Activez ce paramètre pour autoriser l'affichage de notifications lorsque le pare-feu Windows bloque une nouvelle application.

9. Sélectionnez **Enregistrer et publier** lorsque vous avez terminé pour envoyer le profil sur les terminaux.

Profil de kiosque

Configurer un profil de kiosque pour transformer votre terminal Windows Desktop en terminal kiosque multi-applications. Ce profil vous permet de configurer les applications qui s'affichent dans le menu Démarrer du terminal.

Vous pouvez télécharger votre propre fichier XML personnalisé pour configurer le profil de kiosque ou créer votre kiosque dans le cadre du profil. Ce profil ne prend pas en charge les comptes de domaine ou des groupes de domaines. L'utilisateur est un compte d'utilisateur intégré créé par Windows.

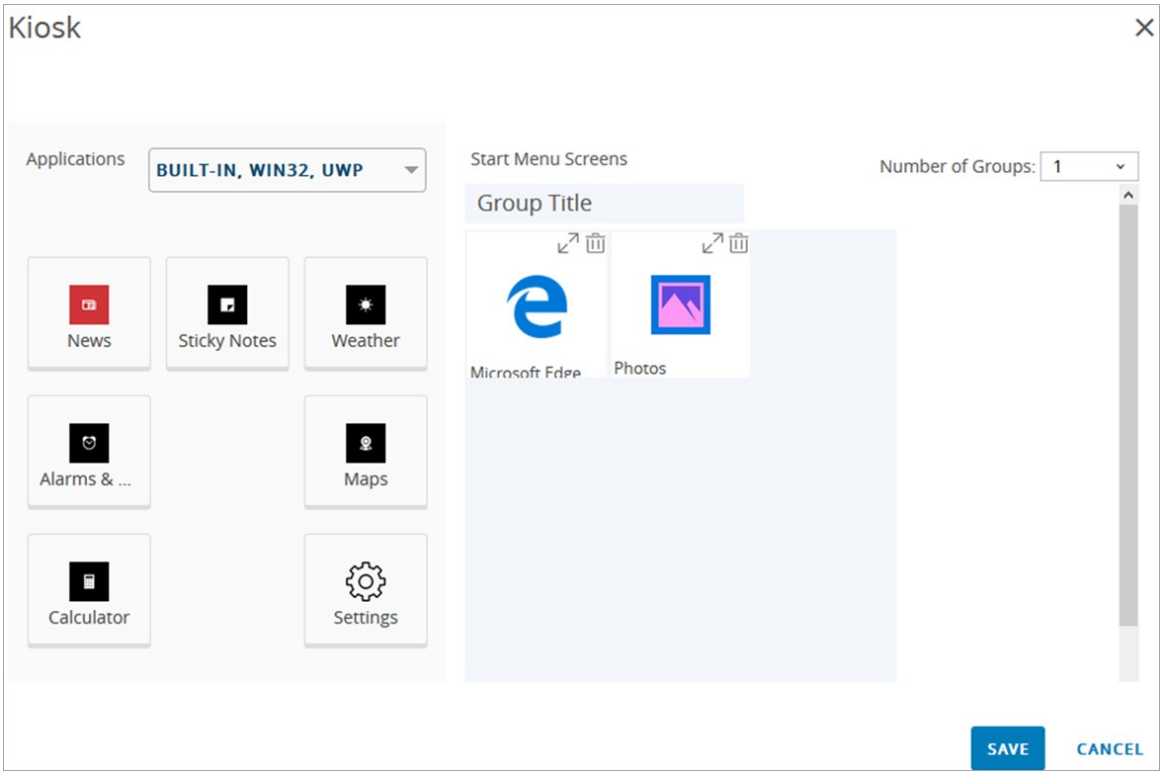
- Applications prises en charge
  - Applications .EXE
    - Les fichiers MSI et ZIP nécessitent que vous ajoutiez le chemin d'accès.
  - Applications intégrées
    - Les applications intégrées sont automatiquement ajoutées au concepteur. Ces applications incluent :
    - Actualités
    - Microsoft Edge
    - Météo
    - Alarmes et horloge
    - Feuillets autocollants
    - Cartes
    - Calculatrice et Photos.

Procédure

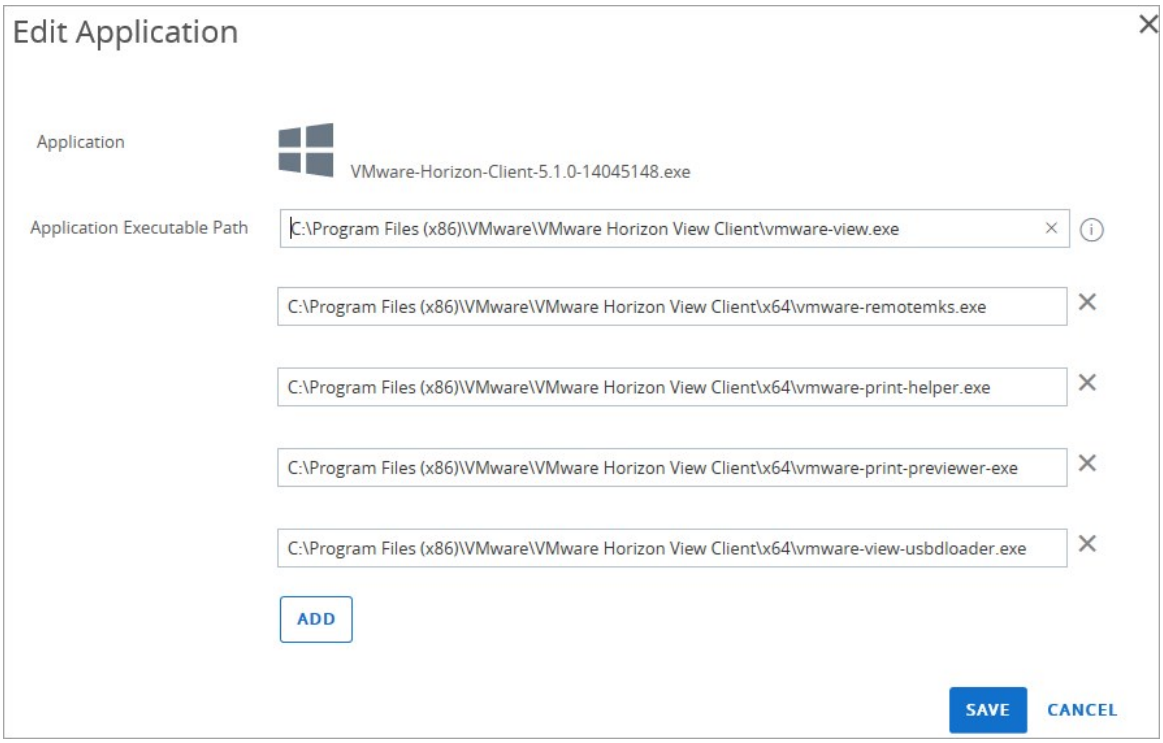
1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil. Vous devez ajouter une attribution avant de configurer le profil de kiosque.
5. Sélectionnez le profil **Kiosque**.

6. Si vous avez déjà votre fichier XML personnalisé, sélectionnez Télécharger le fichier XML du kiosque et complétez les paramètres **Attribuer la configuration d'accès du fichier XML**. Sélectionnez **Télécharger** et ajoutez votre fichier XML de configuration d'accès attribué. Vous pouvez également coller votre code XML dans la zone de texte. Pour plus d'informations, reportez-vous à https://docs.microsoft.com/en-us/windows/client-management/mdm/assignedaccess-csp.
7. Si vous ne disposez pas d'un fichier XML personnalisé, sélectionnez **Créer votre kiosque** et configurez la disposition de l'application.

   Cette disposition est le menu Démarrer du terminal dans une grille. Les applications qui s'affichent sur la gauche sont les applications attribuées au groupe d'attribution que vous avez sélectionné. Certaines applications ont une icône d'engrenage avec un point rouge dans l'angle en haut à droite. Cette icône s'affiche pour les applications qui nécessitent des paramètres supplémentaires lorsqu'elles sont ajoutées à la disposition de kiosque. Après avoir configuré les paramètres, le point rouge disparaît, mais l'icône reste. Vous pouvez sélectionner l'icône de flèche pour modifier la taille des applications. Pour les applications de bureau classiques, vous pouvez uniquement sélectionner Petite ou Moyenne.



   Pour les applications qui nécessitent des applications de support supplémentaires, le profil Kiosque prend en charge l'ajout de ces applications de support à l'aide de l'option Paramètres supplémentaires. Par exemple, VMware Horizon Client nécessite jusqu'à quatre applications de support pour s'exécuter en mode Kiosque. Ajoutez ces applications de support supplémentaires lorsque vous configurez l'application de kiosque principale en ajoutant les valeurs **Chemin exécutable de l'application** supplémentaires.



8. Faites glisser toutes les applications que vous souhaitez ajouter vers le menu Démarrer au centre. Vous pouvez créer jusqu'à quatre groupes pour vos applications. Ces groupes combinent vos applications en sections dans le menu Démarrer.
9. Lorsque vous avez ajouté toutes les applications et les groupes, cliquez sur **Enregistrer**.
10. Sur l'écran Profil du kiosque, sélectionnez **Enregistrer et publier**.

Résultats

Le profil ne s'installe pas sur le terminal tant que toutes les applications incluses dans le profil ne sont pas installées. Une fois que le terminal reçoit le profil, il redémarre et s'exécute en mode Kiosque. Si vous supprimez le profil à partir du terminal, le terminal désactive le mode Kiosque, redémarre et supprime l'utilisateur de kiosque.

Profil de mises à jour OEM

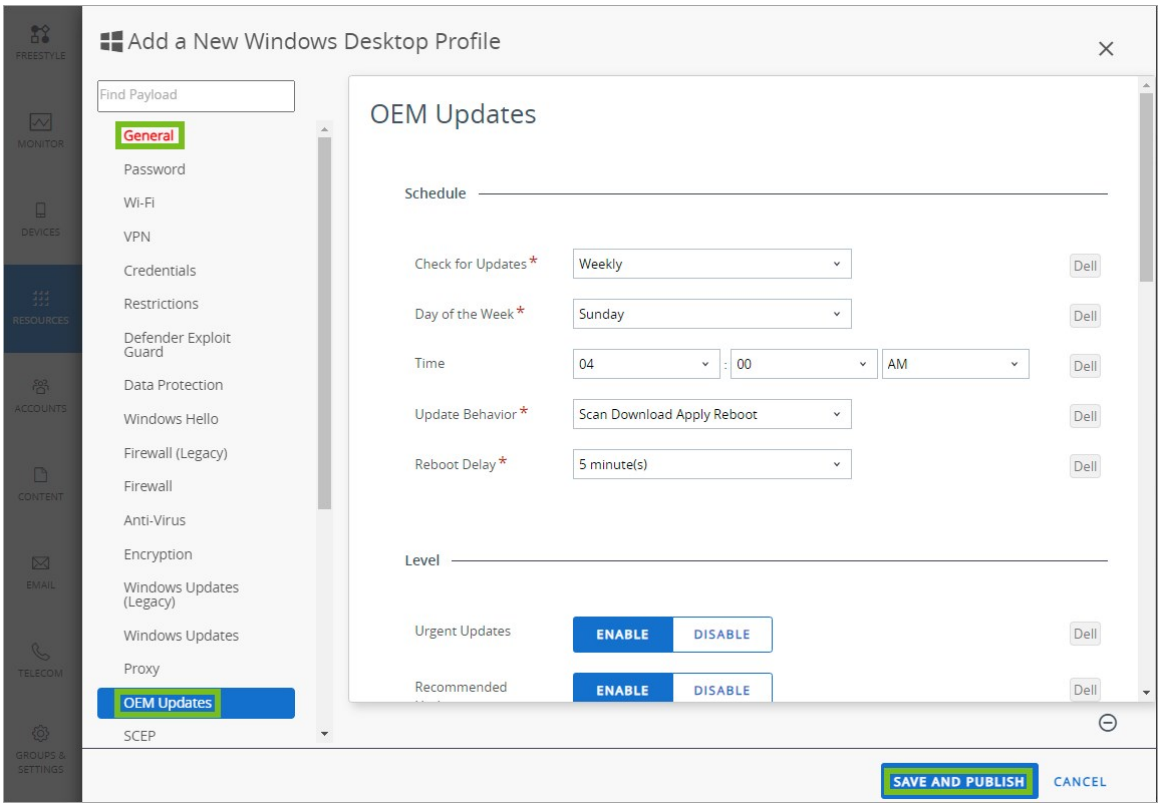
Configurez les paramètres des mises à jour OEM pour des terminaux Dell Enterprise à l'aide du profil Mises à jour OEM. Ce profil nécessite l'intégration à Dell Command | Update.

La prise en charge des paramètres du profil Mises à jour OEM varie selon le terminal Dell Enterprise. Workspace ONE UEM transfère uniquement les paramètres pris en charge par un terminal. Vous pouvez voir toutes les mises à jour OEM déployées sur vos terminaux Windows Desktop sur la page **Mises à jour du terminal**, dans l'onglet **Ressources** > **Mises à jour du terminal** > **Mises à jour OEM**.

Remarque : le profil de mises à jour OEM prend en charge les versions 3.x et ultérieures de Dell Command | Update. La version actuelle de Dell Command | Update est testée avec chaque version de la console.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.

3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.



5. Sélectionnez la section de configuration **Mises à jours OEM** et configurez les paramètres suivants.
    - **Vérifier les mises à jour** : sélectionnez l'intervalle utilisé pour la vérification des mises à jour.
    - **Jour de la semaine** : sélectionnez le jour de la semaine pour la vérification des mises à jour. S'affiche uniquement lorsque l'option **Vérifier les mises à jour** est définie sur **Toutes les semaines**.
    - **Jour du mois** : sélectionnez le jour du mois pour la vérification des mises à jour. S'affiche uniquement lorsque l'option **Vérifier les mises à jour** est définie sur **Tous les mois**.
    - **Heure** : sélectionnez l'heure de la journée pour la vérification des mises à jour.
    - **Comportement de mise à jour** : sélectionnez les actions à effectuer lors de la vérification des mises à jour.
        - Sélectionnez **Rechercher et notifier** pour rechercher les mises à jour et informer l'utilisateur que des mises à jour sont disponibles.
        - Sélectionnez **Rechercher, télécharger et notifier** pour rechercher les mises à jour, télécharger celles qui sont disponibles et informer l'utilisateur que des mises à jour sont disponibles pour être être installées.
        - Sélectionnez **Rechercher, notifier, appliquer et redémarrer** pour rechercher des mises à jour, télécharger celles qui sont disponibles, les installer et redémarrer le terminal.
    - **Délai avant redémarrage** : sélectionnez la durée pendant laquelle le terminal retarde

le redémarrage après avoir téléchargé les mises à jour.

- **Mises à jour urgentes** : sélectionnez **Activer** pour appliquer les mises à jour urgentes au terminal.
- **Mises à jour recommandées** : sélectionnez **Activer** pour appliquer les mises à jour recommandées pour le terminal.
- **Mises à jour facultatives** : sélectionnez **Activer** pour appliquer les mises à jour facultatives au terminal.
- **Pilotes matériels** : sélectionnez **Activer** pour appliquer les mises à jour des pilotes matériels fournies par OEM au terminal.
- **Logiciel d'application** : sélectionnez **Activer** pour appliquer les mises à jour logicielles des applications fournies par OEM au terminal.
- **Mises à jour du BIOS** : sélectionnez **Activer** pour appliquer les mises à jour du BIOS fournies par OEM au terminal. Si les mots de passe du BIOS sont gérés par le profil du BIOS, vous n'aurez pas besoin de désactiver le mot de passe.
- **Mises à jour du microprogramme** : sélectionnez **Activer** pour appliquer les mises à jour du microprogramme fournies par OEM au terminal.
- **Logiciel utilitaire** : sélectionnez **Activer** pour appliquer les mises à jour logicielles des utilitaires fournies par OEM au terminal.
- **Autres** : sélectionnez **Activer** pour appliquer les autres mises à jour fournies par OEM au terminal.
- **Audio** : sélectionnez **Activer** pour appliquer les mises à jour logicielles du terminal audio fournies par OEM au terminal.
- **Puce** : sélectionnez **Activer** pour appliquer les mises à jour logicielles du terminal chipset fournies par OEM au terminal.
- **Entrée** : sélectionnez **Activer** pour appliquer les mises à jour logicielles du terminal d'entrée fournies par OEM au terminal.
- **Réseau** : sélectionnez **Activer** pour appliquer les mises à jour logicielles du terminal réseau fournies par OEM au terminal.
- **Stockage** : sélectionnez **Activer** pour appliquer les mises à jour logicielles du terminal de stockage fournies par OEM au terminal.
- **Vidéo** : sélectionnez **Activer** pour appliquer les mises à jour logicielles du terminal vidéo fournies par OEM au terminal.
- **Autres** : sélectionnez **Activer** pour appliquer les mises à jour logicielles des autres terminaux fournies par OEM au terminal.

6. Cliquez sur **Enregistrer et publier**.

Profil de mot de passe

Utilisez un profil avec mot de passe pour protéger vos terminaux Windows en exigeant un mot de passe à chaque fois qu'ils sortent d'un état inactif. Découvrez comment un profil avec mot de passe avec Workspace ONE UEM garantit que toutes vos informations d'entreprise sensibles sur les

terminaux gérés restent protégées.

Les mots de passe définis à l'aide de ce profil ne prennent effet que si le mot de passe est plus strict que les mots de passe existants. Par exemple, si le mot de passe du compte Microsoft actuel nécessite des paramètres plus stricts que les exigences de section de configuration du Mot de passe, le terminal continue à utiliser le mot de passe du compte Microsoft.

Important : la section de configuration du mot de passe ne s'applique pas aux terminaux joints au domaine.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Mot de passe**.
6. Configurez les paramètres du mot de passe :

Paramètres	Descriptions
Complexité du mot de passe	Définissez votre niveau préféré de complexité de mot de passe sur Simple ou Complexe.
Exiger des caractères alphanumériques	Activez ce paramètre pour exiger un mot de passe de type alphanumérique.
Longueur minimale du mot de passe	Saisissez le nombre minimal de caractères qu'un mot de passe doit contenir.
Durée de vie maximum du mot de passe (en jours)	Saisissez le nombre maximal de jours avant que l'utilisateur ne doive changer le mot de passe.
Durée de vie minimale du mot de passe (jours)	Saisissez le nombre minimal de jours avant que l'utilisateur ne doive changer le mot de passe.
Délai de verrouillage du terminal (min)	Saisissez le nombre de minutes avant que le terminal ne se verrouille automatiquement et que vous deviez ressaisir le mot de passe.

Paramètres	Descriptions
Nombre maximum de tentatives infructueuses	Saisissez le nombre maximal de tentatives avant que le terminal ne doive redémarrer.
Historique du mot de passe (occurrences)	Saisissez le nombre de fois que le mot de passe peut être mémorisé. Si l'utilisateur réutilise un mot de passe inclus dans ces codes d'accès, il ne peut pas réutiliser ce mot de passe. Par exemple, si vous définissez l'historique sur 12, un utilisateur ne peut pas réutiliser les 12 derniers mots de passe.
Faire expirer le mot de passe	Activez ce paramètre pour faire expirer le mot de passe existant sur le terminal et exiger la création d'un nouveau mot de passe. Nécessite l'installation de Workspace ONE Intelligent Hub sur le terminal.
Expiration du mot de passe (jours)	Configurez le nombre de jours pendant lequel un mot de passe est valide avant d'expirer.
Chiffrement réversible pour le stockage des mots de passe	Activez ce paramètre pour que le système d'exploitation stocke les mots de passe à l'aide du chiffrement réversible. Stocker des mots de passe à l'aide du chiffrement réversible est pratiquement identique au stockage de versions de texte brute des mots de passe. Pour cette raison, n'activez pas cette politique à moins que les exigences au niveau de l'application ne prévalent sur la protection des informations de mot de passe.
Utiliser l'Agent de protection pour les terminaux Windows	Activez ce paramètre pour utiliser Workspace ONE Intelligent Hub afin d'appliquer les paramètres du profil Mot de passe au lieu de la fonctionnalité DM native. Activez ce paramètre si vous rencontrez des problèmes lors de l'utilisation de la fonctionnalité DM native.

7. Sélectionnez **Enregistrer et publier** lorsque vous avez terminé pour envoyer le profil sur les terminaux.

Profil Peer Distribution

Workspace ONE Peer Distribution utilise la fonctionnalité Windows BranchCache native intégrée au système d'exploitation Windows. Cette fonctionnalité fournit une technologie pair à pair alternative.

Configurez la distribution pair-à-pair sur vos terminaux Windows avec le profil **Peer Distribution Windows Desktop**. La distribution pair-à-pair prend en charge les modes de BranchCache **Distribué**, **Hébergé** et **Local**, ainsi que leurs paramètres de configuration supplémentaires tels que le pourcentage d'espace disque et la durée de vie maximale du cache. Vous pouvez également afficher les statistiques BranchCache d'une application à partir du panneau Détails de la distribution homologue sous **Applications et livres** > **Natives** > **Affichage en liste** > **Détails de l'application**.

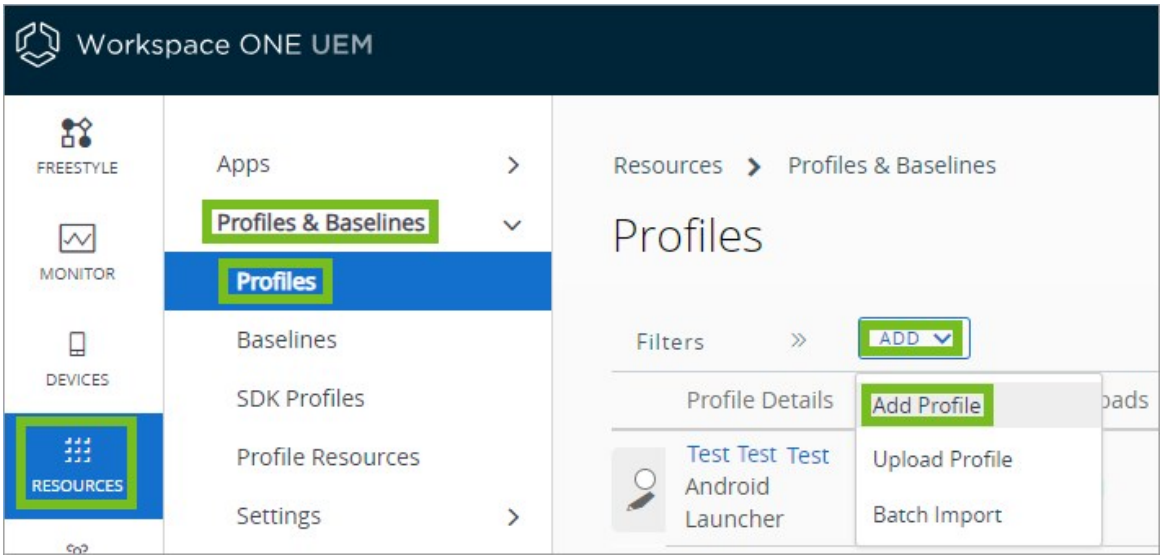
La distribution pair à pair avec Workspace ONE vous permet de déployer vos applications Windows sur des réseaux d'entreprise. Ce profil utilise la fonctionnalité Windows BranchCache native intégrée au système d'exploitation Windows.

Configuration d'un profil Distribution pair à pair

La distribution pair à pair avec Workspace ONE vous permet de déployer vos applications Windows sur des réseaux d'entreprise. Ce profil utilise la fonctionnalité native Windows BranchCache intégrée dans le système d'exploitation Windows.

Pour que vous puissiez utiliser le profil Peer Distribution pour la distribution pair à pair, cette dernière doit répondre à la configuration requise pour Workspace ONE.

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



2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Peer Distribution** puis **Configurer**.

   Vous devez disposer d'un stockage de fichiers configuré avant de pouvoir créer un profil Peer Distribution. Pour plus d'informations, reportez-vous à la section Configuration requise pour Workspace ONE Peer Distribution.

6. Sélectionnez le **Mode Workspace ONE Peer Distribution** à utiliser.

Paramètre	Description
Distribué	Sélectionnez cette option pour que vos terminaux téléchargent des applications depuis des pairs dans un sous-réseau local.
Hébergé	Sélectionnez cette option pour que vos terminaux téléchargent des applications à partir d'un serveur de cache hébergé.
Local	Sélectionnez cette option pour que vos terminaux téléchargent des applications à partir de la mise en cache de terminal local uniquement.
Désactivé	Sélectionnez cette option pour désactiver la distribution pair-à-pair.

7. Configurez les paramètres de **Mise en cache** :

Paramètre	Description

Durée de vie maximale du cache (jours)	Saisissez le nombre maximum de jours pendant lesquels les éléments de distribution pair-à-pair peuvent rester dans le cache avant que le terminal ne les purge.
Pourcentage d'espace disque utilisé pour BranchCache	Saisissez la quantité d'espace disque local que le terminal doit autoriser pour la distribution pair-à-pair.

8. Si vous définissez le mode de distribution sur Hébergé, configurez les paramètres **Serveurs de cache hébergés**. Vous devez ajouter au moins un serveur de cache hébergé depuis et vers lequel les terminaux peuvent télécharger du contenu.
9. Cliquez sur **Enregistrer et publier**.

Profil de personnalisation

Configurez un profil de personnalisation pour les terminaux Windows Desktop afin de configurer les paramètres de personnalisation Windows. Ces paramètres incluent l'arrière-plan du poste de travail et les paramètres du menu Démarrer.

Les options de ce profil sont toutes facultatives. Ne configurez que les paramètres dont vous avez besoin pour répondre à vos besoins de personnalisation.

Ce profil ne crée pas de terminal kiosque multi-applications comme le profil Kiosque.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Personnalisation**.
6. Configurez les paramètres **Images** :

Paramètres	Descriptions
Image de poste de travail	Sélectionnez **Importer** pour ajouter une image à utiliser comme arrière-plan du poste de travail.
Image de l'écran de verrouillage	Sélectionnez **Importer** pour ajouter une image à utiliser comme arrière-plan de l'écran de verrouillage.

7. **Importer** un fichier XML de mise en page de départ. Ce fichier XML remplace la mise en page du menu de démarrage par défaut et empêche les utilisateurs de la modifier. Vous pouvez configurer la disposition des vignettes, le nombre de groupes et les applications dans chaque groupe. Vous devez créer ce fichier XML vous-même. Pour plus d'informations sur la création d'un fichier XML de mise en page de départ, reportez-vous à https://docs.microsoft.com/en-us/windows/configuration/customize-and-export-start-layout.
8. Configurez les paramètres **Stratégies du menu Démarrer**. Ces paramètres vous permettent de contrôler quels raccourcis sont autorisés dans le menu Démarrer. Vous pouvez également choisir de **masquer** ou d'**afficher** certaines options, telles que l'option **Arrêter** ou la **liste des applications**.

9. Cliquez sur **Enregistrer et publier**.

Profil Proxy

Créez un profil Proxy pour configurer un serveur proxy pour vos terminaux Windows Desktop. Ces paramètres ne s'appliquent pas aux connexions VPN.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Proxy** et configurez les paramètres :

Paramètres	Description
Paramètres de détection automatique	Activez cette option pour que le système tente automatiquement de trouver le chemin d'accès à un script de configuration automatique de proxy (PAC).
Utiliser un script de configuration	Activez cette option pour entrer le chemin d'accès au fichier du script PAC.
Adresse de script	Entrez le chemin d'accès au fichier du script PAC. Cette option s'affiche lorsque l'option **Utiliser un script de configuration** est activée.
Utiliser un serveur proxy	Activez cette option pour utiliser un serveur proxy statique pour les connexions Ethernet et Wi-Fi. Ce serveur proxy est utilisé pour tous les protocoles. Ces paramètres ne s'appliquent pas aux connexions VPN.
Adresse du serveur proxy	Entrez l'adresse du serveur proxy. L'adresse doit respecter le format suivant : `<server>[":"<port>]`.
Exceptions	Entrez toutes les adresses qui ne doivent pas utiliser le serveur proxy. Le système n'utilisera pas le serveur proxy pour ces adresses. Séparez les entrées par un point-virgule (;).
Utilisez un proxy pour les adresses locales (intranet)	Activez cette option pour utiliser le serveur proxy pour des adresses locales (intranet).

6. Cliquez sur **Enregistrer et publier**.

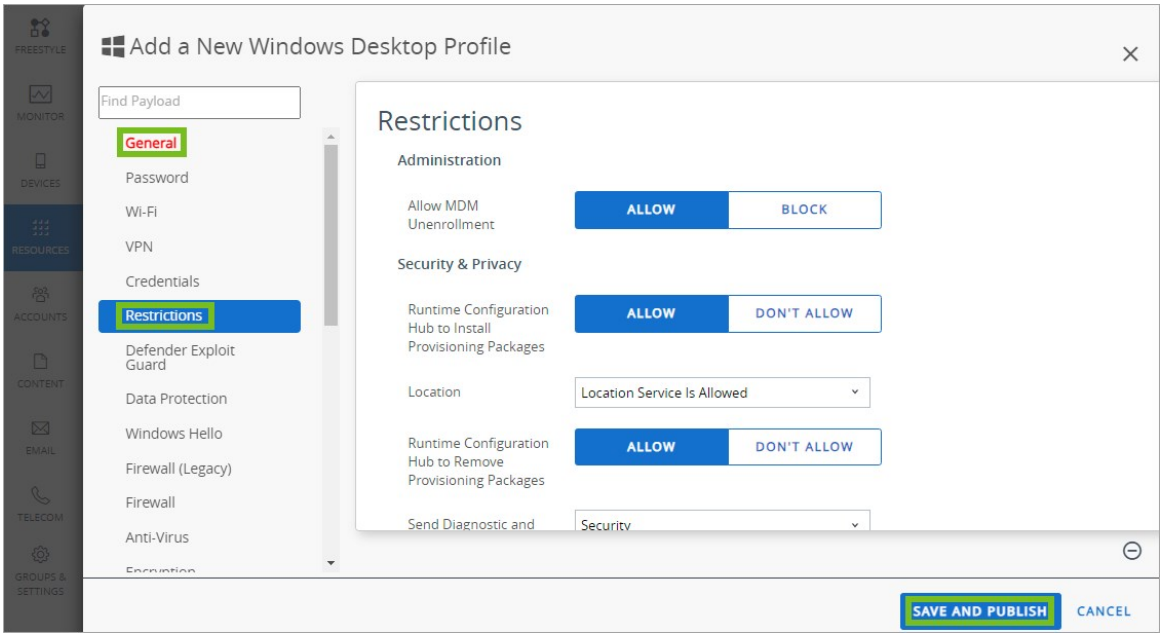
Profil Restrictions

Utilisez les profils Restrictions pour désactiver l'accès des utilisateurs finaux aux fonctionnalités du terminal afin que vos terminaux Windows ne soient pas endommagés. Découvrez comment contrôler les paramètres et options que les utilisateurs finaux peuvent utiliser ou modifier avec le profil de restrictions Workspace ONE UEM.

La version et l'édition de Windows que vous utilisez ont une incidence sur les restrictions qui s'appliquent à un terminal.

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

2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.



5. Sélectionnez le profil **Restrictions**.
6. Configurez les paramètres **Administration** :

Paramètres	Description
Autoriser le désenrôlement MDM manuel	Autorisez l'utilisateur à désenrôler manuellement son terminal de Workspace ONE UEM via l'enrôlement Espace de travail/accès professionnel. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
La configuration en cours du Hub installe les packages de provisionnement.	Activez ce paramètre pour autoriser l'utilisation de packages de déploiement dans le cadre de l'enrôlement de terminaux dans Workspace ONE UEM (déploiement par lots). Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Emplacement	Sélectionnez le fonctionnement des services de localisation sur le terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
La configuration en cours de l'agent supprimera le pack de configuration.	Activez ce paramètre pour autoriser la suppression de packages de déploiement. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Envoyer les données de télémétrie concernant le diagnostic et l'utilisation	Sélectionnez le niveau de données de télémétrie à envoyer à Microsoft. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Exiger un compte Microsoft pour le MDM	Activez ce paramètre pour exiger qu'un compte Microsoft pour les terminaux reçoive les politiques ou les applications.

Paramètres	Description
Exiger un compte Microsoft pour l'installation d'applications modernes	Activez ce paramètre pour exiger qu'un compte Microsoft pour les terminaux télécharge et installe les applications Windows.
Les packs de configuration doivent disposer d'un certificat signé par une autorité de terminaux fiable.	Activez ce paramètre pour exiger un certificat approuvé pour tous les packages de déploiement (déploiement par lots). Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autoriser l'utilisateur à modifier les paramètres Auto Play	Autorisez l'utilisateur à modifier le programme utilisé pour l'Auto Play des types de fichiers. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autorisez l'utilisateur à modifier les paramètres Data Sense.	Autorisez l'utilisateur à modifier les paramètres Data Sense afin de restreindre l'utilisation des données sur le terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Date/heure	Autorisez l'utilisateur à changer les paramètres Date/heure. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Langue	Autorisez l'utilisateur à changer les paramètres de langue. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autoriser l'utilisateur à modifier les paramètres d'alimentation et de mise en veille.	Autorisez l'utilisateur à changer les paramètres d'alimentation et de mise en veille. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Région	Autorisez l'utilisateur à modifier la région. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autorisez l'utilisateur à modifier les options de connexion.	Autorisez l'utilisateur à modifier les options de connexion. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
VPN	Autorisez l'utilisateur à changer les paramètres de VPN. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autoriser l'utilisateur à modifier les paramètres de Workplace	Autorise l'utilisateur à changer les paramètres Workplace et les fonctions MDM sur le terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autoriser l'utilisateur à modifier les paramètres de compte	Autorisez l'utilisateur à modifier les paramètres de compte. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Bluetooth	Autorisez l'utilisation du Bluetooth sur le terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Publicité Bluetooth de terminal	Autorisez le terminal à diffuser les annonces Bluetooth. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Les terminaux compatibles avec Bluetooth peuvent découvrir le terminal	Autorisez la détection du Bluetooth par d'autres terminaux Bluetooth. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.

Paramètres	Description
appareil photo	Autorisez l'accès à la fonction appareil-photo du terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Cortana	Autorisez l'accès à l'application Cortana. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Détection de terminaux UX sur l'écran de verrouillage	Autorisez l'expérience utilisateur de découverte du terminal à détecter des projecteurs et d'autres moniteurs lorsque l'écran de verrouillage est affiché. Lorsque ce paramètre est activé, les raccourcis clavier Win+P et Win+K ne fonctionnent pas. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Journalisation IME	Activez ce paramètre pour autoriser l'utilisateur à activer et à désactiver la journalisation de conversions incorrectes et la sauvegarde de résultats de réglages automatiques vers un fichier et une saisie prédictive basée sur l'historique. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Accès au réseau IME	Activez ce paramètre pour autoriser l'utilisateur à activer l'ouverture du dictionnaire étendu afin qu'il intègre des recherches Internet et fournisse des suggestions de saisie qui n'existent pas dans le dictionnaire local d'un PC. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
SmartScreen	Activez ce paramètre pour autoriser l'utilisateur à utiliser la fonction Microsoft SmartScreen, une fonction de sécurité qui invite l'utilisateur à dessiner des formes sur une image de l'écran pour déverrouiller le terminal. Cette option permet également aux utilisateurs d'utiliser des codes PIN en tant que mot de passe. **Remarque** : une fois la fonction désactivée, vous ne pouvez pas la réactiver via Workspace ONE UEM MDM. Pour la réactiver, vous devez rétablir les paramètres d'usine du terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Rechercher pour utiliser les informations de localisation.	Autorisez la recherche à utiliser les informations d'emplacement de terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Carte de stockage	Activez ce paramètre pour autoriser l'utilisation d'une carte SD et des ports USB de l'appareil. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Paramètres de synchronisation Windows	Autorisez l'utilisateur à synchroniser les paramètres Windows entre terminaux. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Conseils Windows	Autorisez les conseils Windows sur le terminal pour assister l'utilisateur. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Paramètres de contrôle du compte utilisateur	Sélectionnez le niveau de notification envoyé aux utilisateurs lorsqu'une modification apportée au système d'un terminal nécessite une autorisation de l'administrateur.
Autoriser les applications approuvées hors Microsoft Store	Autorisez le téléchargement et l'installation d'applications non approuvées par le Microsoft Store.

Paramètres	Description
Mises à jour automatiques des boutiques d'applications	Activez ce paramètre pour autoriser des applications téléchargées depuis le Microsoft Store à être automatiquement mises à jour lorsque de nouvelles versions sont disponibles. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autoriser le déverrouillage par le développeur	Autorise l'utilisation du paramètre Déverrouillage par le développeur pour charger des versions de test sur les terminaux. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autoriser la diffusion DVR de jeux vidéo	Activez ce paramètre pour autoriser l'enregistrement et la diffusion de jeux sur le terminal. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Autoriser le partage des données entre plusieurs utilisateurs de la même application.	Autorise le partage de données entre plusieurs utilisateurs d'une application. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Restreindre les données d'application au volume système	Restreint les données d'application au même volume que le système d'exploitation en leur interdisant l'accès aux volumes secondaires ou aux supports amovibles. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Restreindre l'installation des applications au lecteur système	Restreint l'installation d'applications au lecteur système en leur interdisant l'accès aux lecteurs secondaires ou aux supports amovibles. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Connexion automatique aux points d'accès Wi-Fi	Activez ce paramètre pour autoriser le terminal à se connecter automatiquement à des points d'accès Wi-Fi à l'aide de l'assistant Wi-Fi. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Données mobiles en itinérance	Activez ce paramètre pour autoriser l'utilisation de données mobiles en itinérance. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Partage Internet	Activez ce paramètre pour autoriser le partage Internet entre terminaux. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Utilisation des données lors de l'itinérance	Activez ce paramètre pour autoriser les utilisateurs à transmettre et recevoir des données lors des déplacements. Cette restriction s'applique à tous les terminaux Windows 10.
VPN sur le réseau mobile	Autorisez l'utilisation d'un VPN lors de connexions de données cellulaires. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Itinérance VPN sur le réseau mobile	Autorisez l'utilisation d'un VPN lors de connexions de données cellulaires en itinérance. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Saisie automatique	Autorisez l'utilisation de remplissage automatique des informations utilisateur. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Cookies	Autorisez l'utilisation de cookies. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Ne pas suivre	Autorisez l'utilisation de demandes DNT. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.

Paramètres	Description
Gestionnaire de mots de passe	Autorisez l'utilisation du gestionnaire de mots de passe. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Pop-ups	Autorisez les fenêtres locales de navigateur. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Suggestions de recherche dans la barre d'adresses	Autorisez l'affichage des suggestions de recherche dans la barre d'adresse. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
SmartScreen	Autorisez l'utilisation du filtre de contenu et d'emplacements malveillants SmartScreen. Cette restriction n'est pas prise en charge pour les terminaux Windows Home Edition.
Envoyez le trafic Internet à Internet Explorer.	Autorisez le trafic Internet à utiliser Internet Explorer. Cette restriction s'applique à tous les terminaux Windows 10.
URL de la liste des sites d'entreprise	Saisissez l'URL d'une liste d'emplacements d'entreprise. Cette restriction s'applique à tous les terminaux Windows 10.

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

Profil SCEP

Les profils SCEP (de protocole d'inscription de certificats simple) permettent d'installer ces certificats en mode silencieux sur des terminaux sans aucune interaction de la part de l'utilisateur.

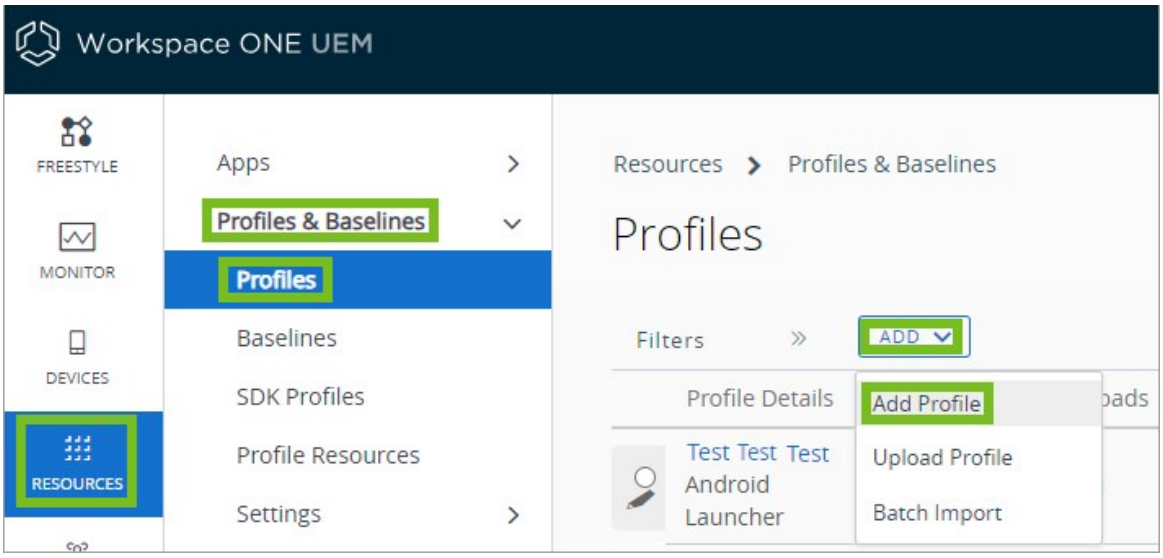
Même avec des mots de passe forts et d'autres restrictions, votre infrastructure reste vulnérable aux attaques par force brute, aux attaques de dictionnaire et aux erreurs des employés. Pour une sécurité renforcée, vous pouvez mettre en place des certificats numériques qui protégeront vos actifs professionnels. Pour installer les certificats sur les terminaux en mode silencieux à l'aide des profils SCEP, vous devez d'abord définir une autorité de certification (CA), puis configurer une section de configuration **SCEP** en plus de votre section de configuration **EAS**, **Wi-Fi** ou **VPN**. Chacune de ces sections de configuration dispose de paramètres pour l'association d'une autorité de certification définie dans la section de configuration SCEP.

Pour envoyer des certificats vers des terminaux, vous devez configurer une section de configuration **SCEP** dans le cadre des profils que vous avez créés pour les paramètres EAS, Wi-Fi et VPN.

Configuration d'un profil SCEP

Un profil SCEP installe les certificats sur les terminaux en mode silencieux pour qu'ils soient utilisés avec l'authentification des terminaux.

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



2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil d'utilisateur** ou **Profil du terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **SCEP**.
6. Configurez les paramètres SCEP, notamment :

Paramètres	Descriptions
Source des identifiants	Ce menu déroulant est toujours réglé sur l'autorité de certification définie.
Autorité de certification	Sélectionnez l'autorité de certification que vous souhaitez utiliser.
Modèle de certificat	Sélectionnez le modèle disponible pour le certificat.
Emplacement de la clé	Sélectionnez l'emplacement de la clé privée du certificat : **TPM si disponible** – Sélectionnez ce paramètre pour stocker la clé privée sur un Module de plateforme sécurisée (TPM) s'il y en a sur le terminal ; dans le cas contraire, stockez-la dans le système d'exploitation. **TPM obligatoire** – Sélectionnez ce paramètre pour stocker la clé privée sur un Module de plateforme sécurisée (TPM). S'il n'y a pas de TPM, le certificat ne peut pas être installé et une erreur s'affiche sur le terminal. **Logiciel** – Sélectionnez ce paramètre pour stocker la clé privée dans le système d'exploitation du terminal. **Passport** – Sélectionnez ce paramètre pour sauvegarder la clé privée dans Microsoft Passport. Cette option nécessite l'intégration d'Azure AD.
Nom du conteneur	Spécifiez le nom du conteneur Passport for Work (maintenant appelé « Windows Hello Entreprise »). Ce paramètre s'affiche lorsque vous définissez **Emplacement de la clé** sur **Passport**.

7. Configurez le profil Wi-Fi, VPN ou EAS.
8. Sélectionnez **Enregistrer et publier** lorsque vous avez terminé d'envoyer le profil aux terminaux.

Profil Mode d'application unique

Le profil Mode d'application unique vous permet de limiter l'accès au terminal à une application unique. Avec le mode d'application unique, le terminal est verrouillé et ouvert à une seule application jusqu'à ce que la section de configuration soit supprimée. La politique est activée après un redémarrage du terminal.

Le mode d'application unique connaît cependant quelques restrictions et limitations.

- Applications Windows universelles ou modernes uniquement. Le mode d'application unique ne prend pas en charge les applications .msi ou .exe héritées.
- Les utilisateurs doivent être des utilisateurs locaux uniquement. Ils ne peuvent être ni utilisateurs de domaine, ni administrateurs, ni issus d'un compte Microsoft, ni invités. L'utilisateur standard doit être un utilisateur local. Les comptes de domaine ne sont pas pris en charge.

Procédure

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil d'utilisateur**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Mode d'application unique**.
6. Configurez les paramètres du **mode Application unique** pour **Nom d'application** et entrez le nom convivial de l'application. Pour les applications Windows, le nom convivial est le nom du module ou l'ID du module. Exécutez une commande PowerShell pour obtenir le nom convivial de l'application installée sur le terminal. La commande « Get-AppxPackage » renvoie le nom convivial de l'application sous « nom ».
7. Après avoir configuré un profil Mode d'application unique, vous devez configurer un mode d'application unique sur le terminal.
    - Une fois le profil Mode d'application unique reçu sur le terminal, redémarrez ce dernier pour commencer.
    - Au redémarrage, un message vous demande de vous connecter au terminal à l'aide du compte de l'utilisateur standard.

Une fois la connexion établie, la politique démarre et le Mode d'application unique est prêt à être utilisé. Si vous devez vous déconnecter du Mode d'application unique, appuyez sur la touche Windows rapidement cinq fois pour lancer l'écran de connexion et vous connecter sous un autre nom d'utilisateur.

Profil VPN

Workspace ONE UEM prend en charge la configuration des paramètres VPN de terminal afin que vos utilisateurs finaux puissent accéder à distance et en toute sécurité au réseau interne de votre organisation. Découvrez comment le profil VPN contrôle les paramètres VPN détaillés, y compris les paramètres de fournisseur VPN spécifiques et l'accès VPN par application.

Important : Avant d'activer le **Verrouillage du VPN**, vérifiez que la configuration du VPN pour le profil VPN fonctionne. Si la configuration du VPN est incorrecte, il est possible que vous ne parveniez pas à supprimer le profil VPN du terminal, car il n'y a pas de connexion Internet.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil d'utilisateur** ou **Profil du terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **VPN**.
6. Configurez les paramètres **Informations de connexion**.
    - **Nom de la connexion** - Entrez le nom de la connexion VPN.
    - **Type de connexion** - Sélectionnez le type de connexion VPN :
    - **Serveur** - Entrez le nom d'hôte ou l'adresse IP du serveur VPN.
    - **Port** - Entrez le port utilisé par le serveur VPN.
    - **Paramètres de connexion avancés** - Activez ce paramètre pour configurer des règles de routage avancées pour la connexion VPN du terminal.
    - **Adresses de routage** - Sélectionnez **Ajouter** pour entrer les adresses IP et la taille du préfixe de sous-réseau du serveur VPN. Vous pouvez ajouter d'autres adresses de routage, en fonction de vos besoins.
    - **Règles de routage DNS** - Sélectionnez Ajouter pour entrer le **Nom de domaine** qui décide quand utiliser le VPN. Saisissez les **Serveurs DNS** et **Serveurs de proxy Web** à utiliser pour chaque domaine spécifique.
    - **Politique de routage** - Choisissez **Forcer tout le trafic via le VPN** ou **Autoriser l'accès direct aux ressources externes**.
        - **Forcer tout le trafic via le VPN** (Forcer Tunnel) : Pour cette règle de trafic, tout le trafic IP doit passer par l'interface VPN uniquement.
        - **Autoriser l'accès direct aux ressources externes** (Scinder Tunnel) : Pour cette règle de filtre du trafic, seul le trafic destiné à l'interface VPN (tel que déterminé par la pile réseau) franchit l'interface. Le trafic Internet peut passer par les autres interfaces.
    - **Proxy** - Sélectionnez **Détection automatique** pour détecter tous les serveurs proxy utilisés par le VPN. Sélectionnez **Manuel** pour configurer le serveur de proxy.
    - **Serveur** - Entrez l'adresse IP du serveur de proxy. Apparaît lorsque le **proxy** est défini sur **Manuel**.
    - **URL de configuration du serveur de proxy** - Entrez l'URL pour les paramètres de configuration du serveur de proxy. Apparaît lorsque le **proxy** est défini sur **Manuel**.
    - **Contournement local du proxy** - Activez ce paramètre pour contourner le serveur de proxy lorsque le terminal détecte qu'il est sur le réseau local.
    - **Protocole** - Sélectionnez le protocole d'authentification à utiliser avec le VPN :

- EAP – Autorise plusieurs méthodes d'authentification.
- Certificat de la machine – Détecte le certificat client dans le magasin de certificats du terminal à utiliser lors de l'authentification.

- **Type EAP**|Sélectionnez le type d'authentification EAP :
  - EAP-TLS – Authentification par carte à puce ou certificat client
  - EAP-MSCHAPv2 – Nom d'utilisateur et mot de passe
  - EAP-TTLS
  - PEAP
  - Configuration personnalisée – Autorise toutes les configurations EAP. Apparaît uniquement si le **protocole** est définir sur **EAP**.
- **Type d'identifiants** - Sélectionnez **Utiliser le certificat** pour utiliser un certificat client. Sélectionnez **Utiliser une carte à puce** afin d'utiliser une carte à puce pour l'authentification. Apparaît lorsque **Type EAP** est défini sur **EAP-TLS**.
- **Sélection de certificat simple** - Activez ce paramètre pour simplifier la liste des certificats que sélectionne l'utilisateur. Les certificats s'affichent, les derniers émis pour chaque entité apparaissent en premier. Apparaît lorsque **Type EAP** est défini sur **EAP-TLS**.
- **Utiliser les identifiants de connexion Windows** - Activez ce paramètre pour utiliser les mêmes identifiants que le terminal Windows. Apparaît lorsque **Type EAP** est défini sur **EAP-MSCHAPv2**.
- **Protection de la confidentialité** - Entrez la valeur à envoyer aux serveurs avant que le client n'authentifie l'identité du serveur. Apparaît lorsque **Type EAP** est défini sur **EAP-TTLS**.
- **Méthode d'authentification interne** - Sélectionnez la méthode d'authentification pour l'authentification d'identité interne. Apparaît lorsque **Type EAP** est défini sur **EAP-TTLS**.
- **Activer la reconnexion rapide** - Activez ce paramètre pour réduire le délai entre une demande d'authentification par un client et la réponse du serveur. Apparaît lorsque **Type EAP** est défini sur **PEAP**.
- **Activer la protection de la confidentialité** - Activez ce paramètre pour protéger l'identité de l'utilisateur jusqu'à ce que le client soit authentifié avec le serveur.
- **Règles du VPN par application** - Sélectionnez **Ajouter** pour ajouter des règles de trafic pour les applications héritées et modernes.
- **ID d'application** - Sélectionnez tout d'abord si l'application est une application de store ou de bureau. Entrez ensuite le chemin d'accès au fichier d'application pour les applications de poste de travail. Vous pouvez également entrer le nom de la famille de packages pour les applications du store pour spécifier l'application à laquelle s'appliquent les règles de trafic.
  - Exemple de chemin d'accès du fichier : %ProgramFiles%/ Internet Explorer/iexplore.exe
  - Nom de famille du pack, par exemple :

AirWatchLLC.AirWatchMDMAgent_htcwkw4rx2gx4 La recherche PFN vous permet de rechercher le PFN d'une application en sélectionnant l'icône **Rechercher**. Une fenêtre d'affichage apparaît vous permettant de sélectionner l'application que vous souhaitez configurer selon les règles VPN par application. Le PFN est ensuite rempli automatiquement.

- **VPN à la demande** - Activez ce paramètre pour que la connexion VPN se connecte automatiquement au lancement de l'application.
- **Politique de routage** - Sélectionnez la politique de routage pour l'application.
  - **Autoriser l'accès direct aux ressources externes** autorise le trafic VPN et le trafic via la connexion au réseau local.
  - **Forcer tout le trafic via le VPN** force tout le trafic via le VPN.
- **Règles de routage DNS** - Activez ce paramètre pour ajouter des règles de routage DNS pour le trafic des applications. Sélectionnez **Ajouter** pour ajouter des **Types de filtre** et des **Valeurs de filtre** pour les règles de routage. Seul le trafic de l'application spécifiée correspondant à ces règles peut être envoyé par VPN.
  - **Adresse IP** : Une liste de valeurs séparées par des virgules spécifiant la plage d'adresses IP distantes à autoriser.
  - **Port** : Une liste de valeurs séparées par des virgules spécifiant les étendues de port distantes à autoriser. Par exemple : 100–120, 200, 300–320. Les ports ne sont pas valides lorsque le protocole est défini sur TCP ou UDP.
  - **Protocole IP** : Valeur numérique entre 0 et 255 indiquant le protocole IP à autoriser. Par exemple, TCP = 6 et UDP = 17.
- **Règles du VPN à l'échelle des terminaux** - Sélectionnez **Ajouter** pour ajouter des règles de trafic pour l'intégralité du terminal. Sélectionnez **Ajouter** pour ajouter des **Types de filtre** et des **Valeurs de filtre** pour les règles de routage. Seul le trafic correspondant à ces règles peut être envoyé par VPN.
  - **Adresse IP** : Une liste de valeurs séparées par des virgules spécifiant la plage d'adresses IP distantes à autoriser.
  - **Port** : Une liste de valeurs séparées par des virgules spécifiant les étendues de port distantes à autoriser. Par exemple : 100–120, 200, 300–320. Les ports ne sont pas valides lorsque le protocole est défini sur TCP ou UDP.
  - **Protocole IP** : Valeur numérique entre 0 et 255 indiquant le protocole IP à autoriser. Par exemple, TCP = 6 et UDP = 17. Pour obtenir la liste des valeurs numériques de tous les protocoles, reportez-vous à https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.
- **Mémoriser les identifiants** - Activez ce paramètre pour mémoriser les informations d'identification.
- **Toujours actif** - Activez ce paramètre pour forcer la connexion VPN à rester toujours active.
- **Verrouillage du VPN** - Activez ce paramètre pour forcer le VPN à rester actif et ne jamais se déconnecter, pour désactiver tout accès réseau si le VPN n'est pas

connecté et, enfin, pour empêcher les autres profils VPN de se connecter sur le terminal. Un profil VPN avec option Verrouillage du VPN activé doit être supprimé pour que vous puissiez envoyer un nouveau profil VPN au terminal. Cette fonctionnalité s'affiche uniquement si le profil est défini sur Contexte de terminal.

- **Contournement local** - Activez ce paramètre pour contourner la connexion VPN pour le trafic Intranet.
- **Détection de réseaux approuvés** - Entrez les adresses des réseaux approuvés, séparées par des virgules. Il n'y a pas de connexion au VPN lorsqu'une connexion réseau approuvée est détectée.
- **Domaine** - Sélectionnez **Ajouter un nouveau domaine** pour ajouter des domaines de résolution via le serveur VMware Tunnel. Tous les domaines ajoutés seront résolus par le biais du serveur VMware Tunnel, quelle que soit l'application à l'origine du trafic. Par exemple, vmware.com est résolu via le serveur VMware Tunnel si vous utilisez les applications Chrome (approuvées) ou Edge (non approuvées). Cette option s'affiche uniquement lorsque vous créez le profil VPN en tant que profil utilisateur.

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

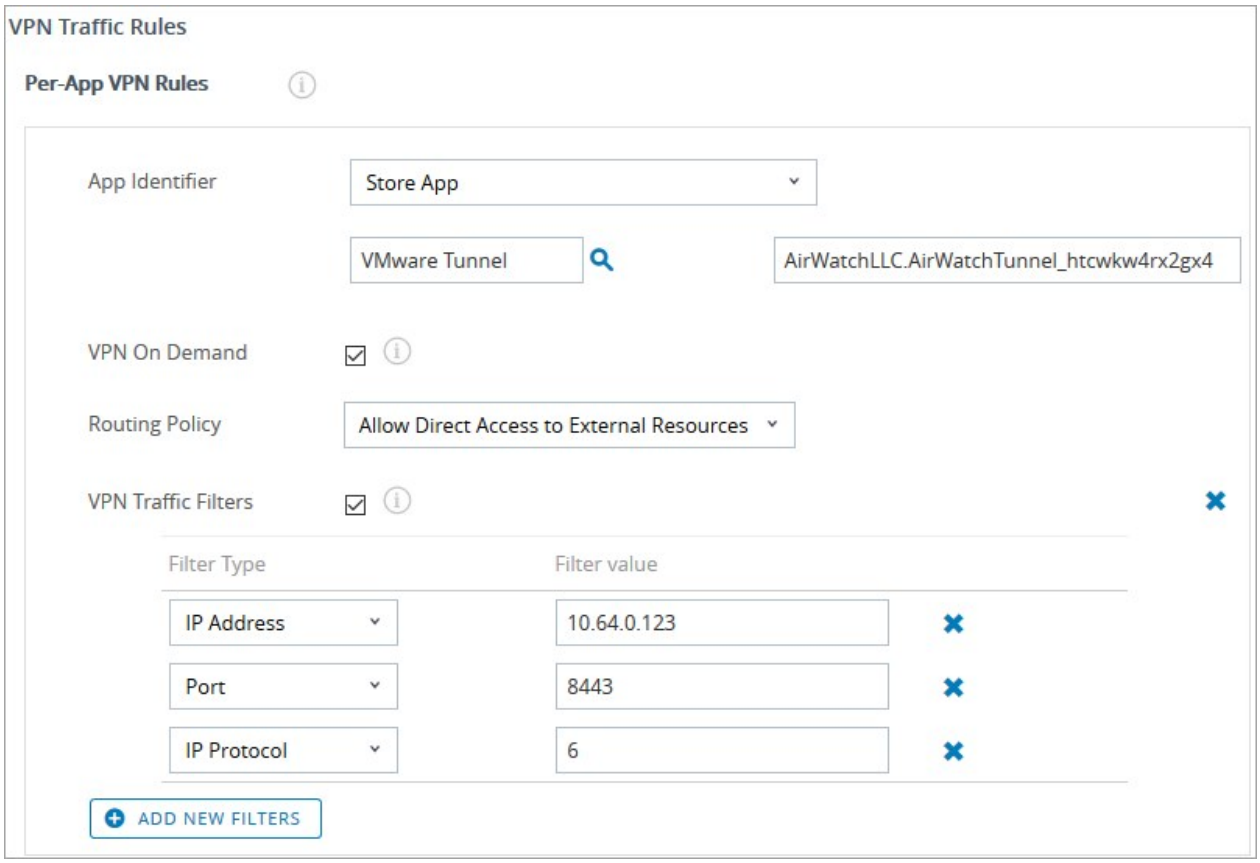
Les profils VPN Workspace ONE UEM prennent en charge la configuration des paramètres VPN par application pour les terminaux Windows. Découvrez comment configurer votre profil VPN pour utiliser les règles de trafic et la logique spécifiques pour activer l'accès VPN par application.

VPN par application pour Windows utilisant le profil VPN

Les profils VPN Workspace ONE UEM prennent en charge la configuration des paramètres VPN par application pour les terminaux Windows. Découvrez comment configurer votre profil VPN pour utiliser les règles de trafic et la logique spécifiques pour activer l'accès VPN par application.

Le VPN par application vous permet de configurer des règles de trafic VPN basées sur certaines applications spécifiques. Une fois configuré, le VPN se connecte automatiquement lorsqu'une application spécifiée démarre et envoie le trafic de l'application, et uniquement de celle-ci, via la connexion VPN. Grâce à cette flexibilité, vous avez la garantie que les données de l'entreprise restent sécurisées, sans limiter l'accès des terminaux à Internet.

Chaque groupe de règles sous la section Règle de VPN par application utilise l'opérateur logique OR. Ainsi, si le trafic correspond à l'une de ces stratégies définies, il est autorisé via le VPN.



Les applications pour lesquelles les règles de trafic VPN par application s'appliquent peuvent être des applications Windows héritées, telles que les fichiers EXE ou les applications modernes téléchargées du Microsoft Store. En définissant les applications spécifiques pouvant démarrer et utiliser la connexion VPN, le VPN est utilisé uniquement pour le trafic issu de ces applications, pas pour tout le trafic des terminaux. Cette logique permet de sécuriser les données d'entreprise tout en réduisant la bande passante transmise via votre VPN.

Pour vous aider à réduire les contraintes liées à la bande passante du VPN, vous pouvez définir des règles de routage DNS pour la connexion VPN par application. Ces règles de routage limitent la quantité de trafic envoyé via le VPN au seul trafic correspondant à ces règles. Les règles de logique utilisent l'opérateur AND. Si vous définissez une adresse IP, un port et un protocole IP, le trafic devra correspondre à chacun de ces filtres pour passer par le VPN.

Le VPN par application vous permet de configurer un contrôle détaillé des connexions VPN pour chaque application.

Profil Raccourcis Internet

La configuration d'un profil Raccourcis Internet vous permet de déployer des URL vers les terminaux des utilisateurs afin de faciliter l'accès aux sites Web importants.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil d'utilisateur**.
4. Configurez les **paramètres généraux** du profil.

5. Sélectionnez le profil **Raccourcis Internet**.
6. Configurez les paramètres des raccourcis Internet, notamment :

Paramètres	Description
Libellé	Saisissez la description du raccourci Internet.
URL	Saisissez l'URL cible du raccourci Internet.
Afficher dans l'App Catalog	Autorisez l'affichage du raccourci Internet dans l'App Catalog.

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

Profil Wi-Fi

Créez un profil Wi-Fi avec Workspace ONE UEM pour connecter les terminaux à des réseaux d'entreprise masqués, chiffrés ou protégés par mot de passe. Découvrez en quoi les profils Wi-Fi sont utiles pour les utilisateurs qui doivent accéder à plusieurs réseaux et également pour la configuration des terminaux afin qu'ils se connectent automatiquement au réseau sans fil approprié.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Wi-Fi** et configurez les paramètres.

Paramètres	Descriptions
Identifiant SSID	Entrez un identifiant pour le nom (SSID) du réseau Wi-Fi souhaité. Le réseau SSID ne peut pas contenir d'espaces.
Réseau masqué	Activez cette option si le réseau utilise un SSID masqué.
Rejoindre automatiquement	Activez cette option pour que le terminal rejoigne le réseau automatiquement.
Type de sécurité	Utilisez le menu déroulant pour sélectionner le type de sécurité (par exemple, WPA2 personnel) pour le réseau Wi-Fi.
Chiffrement	Utilisez le menu déroulant pour sélectionner le type de chiffrement utilisé. Apparaît en fonction du **Type de sécurité**.
Mot de passe	Saisissez le mot de passe requis pour rejoindre le réseau Wi-Fi (pour les réseaux avec mots de passe statiques). Cochez la case Afficher les caractères pour désactiver les caractères masqués dans la zone de texte. Apparaît en fonction du **Type de sécurité**.
Proxy	Activez cette option pour configurer les paramètres proxy pour la connexion Wi-Fi.
URL	Saisissez l'URL du proxy.

Paramètres	Descriptions
Port	Saisissez le port du proxy.
Protocoles	Sélectionnez le type de protocoles à utiliser : **Certificat** : PEAP-MsChapv2 **EAP-TTLS** : Personnalisé Cette section apparaît lorsque le **Type de sécurité** est défini sur WPA Enterprise ou WPA2 Enterprise.
Authentification interne	Sélectionnez la méthode d'authentification via EAP-TTLS : Nom d'utilisateur/Mot de passe Certificat Cette section apparaît lorsque l'option **Protocoles** est définie sur EAP-TTLS ou PEAP-MsChapv2.
Exiger une liaison de chiffrement	Activez cette option pour exiger une liaison de chiffrement sur les deux authentifications. Cet élément de menu limite les attaques de l'intercepteur.
Utiliser les identifiants de connexion Windows	Activez cette option pour utiliser les informations d'identification de connexion Windows nom d'utilisateur/mot de passe pour s'authentifier. Apparaît lorsque **Nom d'utilisateur/mot de passe** est défini sur **Identité interne**.
Certificat d'identité	Sélectionnez un certificat d'identité que vous pourrez configurer à l'aide de la section de configuration Identifiants. Apparaît lorsque **Certificat** est défini sur **Identité interne**.
Certificats approuvés	Sélectionnez **Ajouter** pour ajouter des certificats approuvés au profil Wi-Fi. Cette section apparaît lorsque le **Type de sécurité** est défini sur WPA Enterprise ou WPA2 Enterprise.
Autoriser les exceptions de fiabilité	Activez ce paramètre pour autoriser des décisions approuvées émanant de l'utilisateur via une boîte de dialogue.

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

Profil Windows Hello

Windows Hello fournit une solution alternative à l'utilisation de mots de passe. Le profil Windows Hello permet de configurer Windows Hello for Business pour vos terminaux Windows Desktop afin que les utilisateurs finaux puissent accéder à vos données sans envoyer de mot de passe.

La protection de terminaux et de comptes à l'aide d'un nom d'utilisateur et d'un mot de passe crée parfois des exploits de sécurité potentiels. Il arrive que des utilisateurs oublient un mot de passe, ou le partagent avec des personnes étrangères à l'entreprise, mettant en danger les données de votre société. Grâce à Windows Hello, les terminaux Windows peuvent s'authentifier en toute sécurité pour accéder à des applications, sites Web et réseaux pour le compte de l'utilisateur, sans envoyer

de mot de passe. Il devient inutile de se souvenir des mots de passe, sans compter qu'en leur absence, les attaques de type MITM risquent moins de compromettre votre sécurité.

Avec Windows Hello, les utilisateurs doivent veiller à disposer d'un terminal Windows avant de s'authentifier via un code PIN ou par le biais de la vérification biométrique Windows Hello. Une fois authentifié avec Windows Hello, le terminal obtient un accès immédiat aux sites Web, applications et réseaux.

Important : Windows Hello for Business nécessite l'intégration d'Azure AD pour fonctionner.

Créez un profil Windows Hello pour configurer Windows Hello for Business pour vos terminaux Windows Desktop afin que les utilisateurs finaux puissent accéder à vos applications, sites Web et réseaux sans saisir de mot de passe.

Création d'un profil Windows Hello

Créez un profil Windows Hello pour configurer Windows Hello for Business pour vos terminaux Windows Desktop afin que les utilisateurs finaux puissent accéder à vos applications, sites Web et réseaux sans saisir de mot de passe.

Important : les profils Windows Hello ne s'appliquent qu'aux terminaux enrôlés par l'intégration d'Azure AD.

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Windows Hello** et configurez les paramètres suivants :

Paramètres	Descriptions
Geste biométrique	Activez ce paramètre pour permettre aux utilisateurs d'utiliser les lecteurs biométriques du terminal.
TPM	Sélectionnez Exiger pour désactiver l'utilisation de Passport sans module TPM installé sur le terminal.
Longueur minimale du code PIN	Saisissez le nombre minimal de chiffres que doit contenir le code PIN.
Longueur maximale du code PIN	Saisissez le nombre maximal de chiffres que doit contenir le code PIN.
Chiffres	Définissez le niveau d'autorisation pour utiliser des chiffres dans le code PIN.
Majuscules	Définissez le niveau d'autorisation pour utiliser des majuscules dans le code PIN.
Minuscules	Définissez le niveau d'autorisation pour utiliser des minuscules dans le code PIN.
Caractères spéciaux	Définissez le niveau d'autorisation pour utiliser des caractères spéciaux dans le code PIN. `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ { | } ~`

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

Profil Gestion des licences Windows

Configurez un profil Gestion des licences Windows pour fournir aux terminaux Windows une clé de licence Windows Entreprise ou Windows Éducation. Utilisez ce profil pour mettre à niveau les terminaux qui ne disposent pas de Windows Entreprise.

Important :

Cette mise à niveau est irréversible. Si vous publiez ce profil sur des terminaux personnels, vous ne pouvez pas supprimer la gestion des licences par MDM. Windows ne peut effectuer la mise à niveau que dans les configurations suivantes :

- Windows Entreprise à Windows Éducation
- Windows Famille à Windows Éducation
- Windows Professionnel à Windows Éducation
- Windows Professionnel à Windows Entreprise

Procédure

1. Accédez à > **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Sélectionnez **Windows**, puis **Windows Desktop**.
3. Sélectionnez **Profil de terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **Gestion des licences Windows** et configurez les paramètres suivants :

Paramètres	Descriptions
Édition Windows	Sélectionnez l'édition **Entreprise** ou **Éducation**.
Saisissez une clé de licence valide	Saisissez la clé de licence correspondant à l'édition de Windows que vous utilisez.

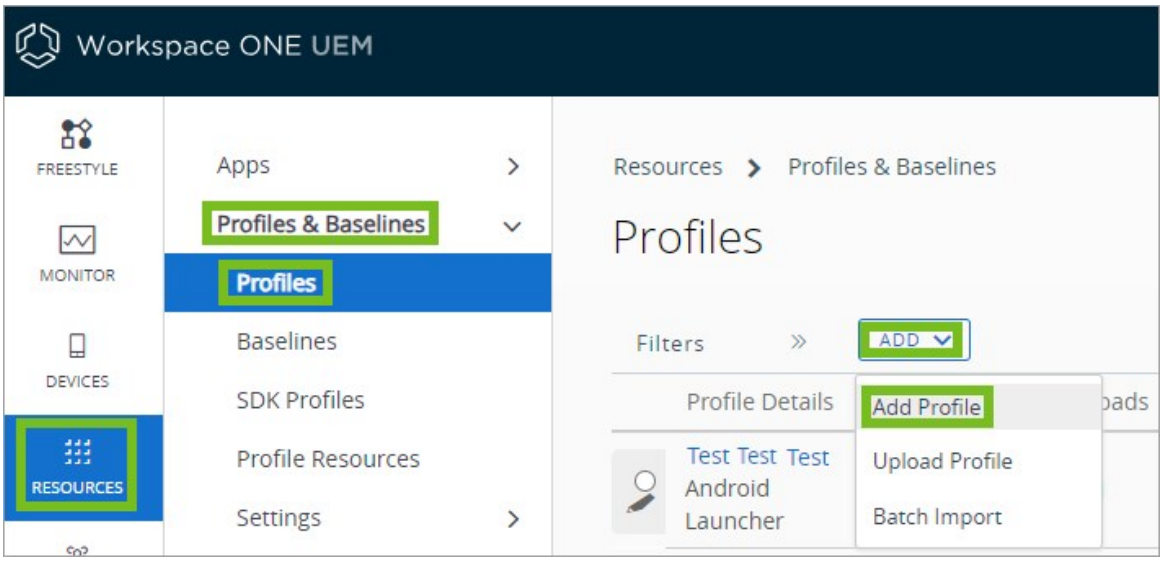
6. Cliquez sur **Enregistrer et publier** pour envoyer le profil vers les terminaux.

Profil Mises à jour Windows

Créez un profil Mises à jour Windows vous permet de configurer les paramètres des mises à jour Windows sur les terminaux Windows Desktop en utilisant Windows 10, 2004 et versions ultérieures. Ce profil présente plus d'améliorations et de fonctionnalités supplémentaires que le profil de mise à jour Windows (hérité). L'utilisation de la version mise à jour garantit que tous vos terminaux sont à jour et pourront tirer parti des nouvelles fonctionnalités ajoutées à la console, tout en améliorant la sécurité des terminaux et du réseau.

Pour créer ou configurer un profil de mises à jour Windows, utilisez le gestionnaire de périphériques Windows.

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



2. Choisissez **Windows** > **Windows Desktop** > **Profil de terminal**.
3. Dans **Profil de terminal**, sélectionnez **Mises à jour Windows** puis cliquez sur le bouton pour le **Configurer**.
4. Une fois configurés, vous pouvez personnaliser les paramètres si nécessaire. Ce tableau fournit plus d'informations sur ce que chaque paramètre est censé faire.

Paramètre	Description
Définition	
Source de mise à jour Windows	Sélectionnez la source des mises à jour Windows. **Service de mise à jour Microsoft** – Sélectionnez cette option pour utiliser le serveur de mises à jour Microsoft par défaut. **WSUS professionnel** – Sélectionnez cette option pour utiliser un serveur d'entreprise et entrez l'URL du serveur WSUS et le Groupe WSUS. Le terminal doit contacter le WSUS au moins une fois pour que ce paramètre prenne effet. Si vous sélectionnez WSUS professionnel comme source, votre administrateur informatique pourra visualiser les mises à jour installées et le statut des terminaux dans le groupe WSUS. Remarque : La source ne peut pas être modifiée après sa définition.
Branche de mise à jour	Sélectionnez la branche à suivre pour les mises à jour. **Windows Insider - Canal Dev** – Les builds Insider Preview dans ce canal sont publiées environ une fois par semaine et contiennent les toutes dernières fonctionnalités. Cela en fait l'idéal pour l'exploration des fonctionnalités.) **Windows Insider - Canal Bêta** – Les builds Insider Preview dans ce canal sont publiées environ une fois par mois et sont plus stables que les versions Fast Ring, ce qui les rend mieux adaptées à des fins de validation. **Windows Insider - Canal d'aperçu de la version** – Les builds Insider Preview dans ce canal sont les versions GA presque terminées pour valider la prochaine version GA. **Canal de disponibilité général (ciblé)** – Il n'existe aucun aperçu des fonctionnalités et les mises à jour des fonctionnalités sont publiées annuellement.

Paramètre	Description
Gérer les builds d'aperçu	Sélectionnez l'accès pour prévisualiser les builds. Si vous souhaitez exécuter un terminal dans Insider Preview, assurez-vous que cette option est définie sur « Activer les builds d'aperçu » : **Désactiver les builds d'aperçu** **Désactiver les builds d'aperçu une fois que la version suivante est publique** **Activer les builds d'aperçu**
Planification du terminal	
Activer la planification des terminaux	Lorsque cette option est activée, vous pouvez définir la manière dont les terminaux gèrent la planification de l'installation des mises à jour et du redémarrage automatique (forcé). Lorsque cette option est activée, vous verrez plus d'options pour configurer le comportement de mise à jour automatique, définir les heures d'activité et configurer le nombre de jours dont disposeront les utilisateurs avant que les mises à jour ne soient automatiquement envoyées à leurs terminaux.
Comportement de mise à jour	
Activer le comportement de mise à jour	Lorsque cette option est activée, vous pouvez définir les types de mises à jour proposées et le moment auquel les terminaux éligibles les recevront. Lorsque cette option est activée, vous verrez plus d'options pour désactiver la double analyse, autoriser les mises à jour de l'application Microsoft, définir la durée de report d'une mise à jour de fonctionnalité et exclure des pilotes Windows et/ou désactiver Safe Guard.
Comportement du terminal	
Activer le comportement du terminal	Lorsque cette option est activée, vous pouvez définir la manière dont les configurations du comportement de mise à jour sont gérées par le terminal. Lorsque cette option est activée, vous verrez plus d'options pour autoriser les mises à jour automatique Windows à télécharger sur des réseaux mesurés, à ignorer les limites de téléchargement des données cellulaires pour les mises à jour des applications et ignorer les limites de téléchargement des données cellulaires pour les mises à jour système.
Optimisation de la distribution	
Activer l'optimisation de la distribution	Lorsque cette option est activée, vous pouvez définir comment réduire la consommation de bande passante. Lorsque cette option est activée, vous verrez plus d'options pour sélectionner les options Mode de téléchargement, Source de l'hôte du cache, Source de l'ID de groupe, Source HTTP, Source du serveur de cache, Réseau, Configuration requise du terminal et Limitation de bande passante réseau.
Version du système d'exploitation	

Paramètre	Description
Version du système d'exploitation	Lorsque cette option est activée, vous pouvez spécifier la version cible et la version du produit cible qui doivent être déplacées ou doivent rester jusqu'à la fin du service.

5. Une fois que vous avez terminé la personnalisation du profil, n'oubliez pas de sélectionner **Enregistrer et publier** pour envoyer le profil sur vos terminaux.

Dépannage concernant les mises à jour de fonctionnalités et de qualité

Étant donné que les mises à jour Windows peuvent entraîner des problèmes avec des pilotes ou des applications spécifiques, trois boutons ont été ajoutés pour aider à dépanner ces situations. Le bouton **Pause** vous permet de suspendre les mises à jour de fonctionnalités et de qualité avant leur sortie (mais uniquement pendant 35 jours). Le bouton **Restauration** permet de revenir temporairement à la version précédent les mises à jour effectuées qui ont causé des problèmes imprévus, le temps que vous résolviez le problème. Le bouton **Reprendre** active à nouveau la recherche et l'installation des mises à jour Windows.

Profil de mises à jour Windows (héritées)

Le profil de mises à jour Windows (héritées) est destiné aux terminaux Windows Desktop utilisant Windows 10, 1909 ou une version antérieure. Envisagez de migrer ou d'utiliser le nouveau profil de mise à jour Windows pour bénéficier des nouvelles fonctionnalités et améliorations apportées après 2004. Le profil garantit que tous les terminaux sont à jour, ce qui améliore la sécurité des terminaux et du serveur.

Important : Pour afficher la version du système d'exploitation que prend en charge chaque branche de mise à jour, consultez la documentation de Microsoft sur les informations de version de Windows : https://technet.microsoft.com/en-us/windows/release-info.aspx.

Pour créer ou configurer un profil de mises à jour Windows héritées, utilisez le gestionnaire de périphériques Windows.

1. Accédez à > **Terminaux** > **Profils et ressources** > **Profils** > **Ajouter** et sélectionnez **Ajouter un profil**.
2. Choisissez **Windows** > **Windows Desktop** > **Profil de terminal**.
3. Dans **Profil de terminal**, vous verrez un menu d'éléments que vous pouvez personnaliser. Sélectionnez **Mises à jour Windows (héritées)** , puis cliquez sur le bouton pour **Configurer** les paramètres.

Remarque : Vous pouvez remarquer une alerte qui vous informe de la possibilité de migrer des profils existants vers la nouvelle version. Vous pouvez utiliser le bouton **Migrer** pour migrer vos paramètres vers le nouveau profil de mises à jour Windows si vous le souhaitez. Sachez que si vous migrez les profils, certains paramètres ont été améliorés et mis à jour, ce qui entraîne la fin de validité de certaines des anciennes options. Ces modifications ne seront pas migrées à partir des versions précédentes.

1. Après la configuration, vous pouvez personnaliser les paramètres d'un profil hérité (de

nouveau pour les Windows 10, 2004 ou versions antérieures). Ce tableau fournit plus d'informations sur ce que chaque paramètre est censé faire.

Paramètres	Descriptions
Branches et reports	
Source de mise à jour Windows	Sélectionnez la source des mises à jour Windows. **Service de mise à jour Microsoft** – Sélectionnez cette option pour utiliser le serveur de mises à jour Microsoft par défaut. **WSUS professionnel** – Sélectionnez cette option pour utiliser un serveur d'entreprise et entrez l'URL du serveur WSUS et le Groupe WSUS. Le terminal doit contacter le WSUS au moins une fois pour que ce paramètre prenne effet. Si vous sélectionnez WSUS professionnel comme source, votre administrateur informatique pourra visualiser les mises à jour installées et le statut des terminaux dans le groupe WSUS.
Branche de mise à jour	Sélectionnez la branche à suivre pour les mises à jour. Canal semi-annuel Branche Windows Insider - Rapide (Moins stable, Build de développement) Branche Windows Insider - Lente (Plus stable, Build de développement) Insider - Release (Plus stable, Build publique)
Builds Insider	Autorisez le téléchargement de builds Windows Insider de Windows. NON autorisé : Ajout à Windows 10 version 1709 pour spécifier s'il faut autoriser l'accès aux builds Insider Preview de Windows 10.
Différer la période de mises à jour des fonctionnalités (en jours)	Sélectionnez le nombre de jours pendant lesquels différer la mise à jour des fonctionnalités avant d'installer les mises à jour sur le terminal. Le nombre maximal de jours de report d'une mise à jour a changé sous Windows version 1703. Les terminaux exécutant une version antérieure à 1703 peuvent uniquement les différer pendant 180 jours. Les terminaux exécutant une version ultérieure à 1703 peuvent les différer jusqu'à 365 jours. Si vous différez une mise à jour de plus de 180 jours et que vous envoyez le profil vers un terminal exécutant une version de Windows antérieure à la mise à jour 1703, l'installation du profil sur le terminal échoue.
Mettre en pause les mises à jour des fonctionnalités	Activez ce paramètre pour mettre en pause toutes les mises à jour des fonctionnalités pendant 60 jours ou jusqu'à ce que le paramètre soit désactivé. Ce paramètre remplace le paramètre **Différer la période de mises à jour des fonctionnalités (en jours)**. Utilisez cette option pour retarder une mise à jour qui pose problème et qui pourrait s'installer normalement selon vos paramètres de report.
Différer les mises à jour de qualité (en jours)	Sélectionnez le nombre de jours pendant lesquels différer la mise à jour qualité avant d'installer les mises à jour sur le terminal.

Paramètres	Descriptions
Mettre les mises à jour qualité en pause	Activez ce paramètre pour mettre en pause toutes les mises à jour qualité pendant 60 jours ou jusqu'à ce que le paramètre soit désactivé. Ce paramètre remplace le paramètre **Différer la période de mises à jour qualité (en jours)**. Utilisez cette option pour retarder une mise à jour qui pose problème et qui pourrait s'installer normalement selon vos paramètres de report.
Activer les paramètres pour les versions précédentes de Windows	Sélectionnez cette option pour activer les paramètres d'échelonnement pour des versions précédentes de Windows. Ce paramètre active les fonctionnalités de report pour les anciennes versions de Windows 10 telles que 1511 et versions antérieures. Elles ont été modifiées dans la mise à jour anniversaire 1607 dans les paramètres actuels.
Mettre à jour le comportement de l'installation	
Mises à jour automatiques	Définissez comment gérer les mises à jour de la **Branche de mises à jour** sélectionnée : Installer les mises à jour automatiquement (recommandé). Installer les mises à jour automatiquement, mais laisser l'utilisateur planifier le redémarrage de l'ordinateur. Installer les mises à jour automatiquement et recommencer à une heure précise Installer les mises à jour automatiquement et empêcher l'utilisateur de modifier les paramètres du panneau de contrôle Vérifier les mises à jour, mais laisser l'utilisateur décider de leur téléchargement et de leur installation Ne jamais vérifier les mises à jour (non recommandé).
Nombre maximal d'heures d'activité (heures)	Entrez le nombre maximal d'heures d'activité qui empêchent le redémarrage du système en raison de mises à jour.
Heure de début de la période d'activité	Saisissez l'heure de début de la période d'activité. Définissez la période d'activité afin d'empêcher le système de redémarrer durant ces heures.
Heure de fin de la période d'activité	Affiche l'heure de fin de la période d'activité Cette durée est déterminée par les valeurs spécifiées pour **Heure de début de la période d'activité** et **Nombre maximal d'heures d'activité**.
Délais de redémarrage automatique des mises à jour de qualité	Définissez le nombre maximal de jours pouvant s'écouler après l'installation d'une mise à jour qualité ou fonctionnalité avant le redémarrage du système.
Délais de redémarrage automatique des mises à jour de fonctionnalité	Définissez le nombre maximal de jours pouvant s'écouler après l'installation d'une mise à jour de fonctionnalité avant le redémarrage du système.
Notifications de redémarrage automatique (minutes)	Sélectionnez le nombre de minutes d'affichage d'un avertissement avant un redémarrage automatique.

Paramètres	Descriptions
Notification de redémarrage automatique requis	Définissez comment une notification de redémarrage automatique doit être ignorée. **Rejet automatique** : automatiquement rejeté **Rejet par l'utilisateur** : exige de l'utilisateur qu'il ferme la notification.
Délai de redémarrage amorcé des mises à jour de qualité	Les redémarrages amorcés permettent de gérer l'échéance du redémarrage du terminal après l'installation d'une mise à jour qualité ou fonctionnalité pendant les heures actives. Utilisez cette option pour définir le nombre de jours pendant lesquels un utilisateur peut amorcer un redémarrage avant qu'un redémarrage ne soit automatiquement planifié en dehors des heures actives.
Délai de redémarrage amorcé des mises à jour de fonctionnalité	Les redémarrages amorcés permettent de gérer l'échéance du redémarrage du terminal après l'installation d'une mise à jour de fonctionnalité pendant les heures actives. Utilisez cette option pour définir le nombre de jours pendant lesquels un utilisateur peut amorcer un redémarrage avant qu'un redémarrage ne soit automatiquement planifié en dehors des heures actives.
Planification des répétitions de redémarrage amorcé des mises à jour de qualité	Entrez le nombre de jours durant lesquels un utilisateur peut repousser un redémarrage amorcé. Lorsque la période de répétition est écoulée, une heure de redémarrage est planifiée en dehors des heures d'activité.
Planification des répétitions de redémarrage amorcé des mises à jour de fonctionnalité	Entrez le nombre de jours durant lesquels un utilisateur peut repousser un redémarrage amorcé. Lorsque la période de répétition est écoulée, une heure de redémarrage est planifiée en dehors des heures d'activité.
Avertissement de redémarrage planifié (heures)	Sélectionnez le nombre d'heures durant lesquelles un avertissement aux utilisateurs s'affiche avant un redémarrage planifié.
Avertissement de redémarrage planifié (minutes)	Sélectionnez le nombre de minutes durant lesquelles un avertissement aux utilisateurs s'affiche avant un redémarrage planifié.
Avertissement de redémarrage planifié imminent (minutes)	Sélectionnez le nombre de minutes durant lesquelles un avertissement aux utilisateurs s'affiche avant un redémarrage planifié imminent.
Politiques de mise à jour	
Autoriser les mises à jour publiques	Autorisez les mises à jour provenant du service public Windows Update. Le fait de ne pas autoriser ce service risque de créer des problèmes avec le Microsoft Store.
Autoriser les mises à jour Microsoft	Autorisez les mises à jour provenant de Microsoft Update.
Fréquence d'analyse des mises à jour (heures)	Définissez le nombre d'heures entre les analyses de mises à jour.

Paramètres	Descriptions
Dual Scan	Activez cette option afin d'utiliser Windows Update comme source de mise à jour principale lorsque vous avez recours à Windows Server Update Services pour fournir tout le contenu.
Exclure les pilotes Windows Update des mises à jour qualité	Activez cette option pour empêcher l'installation automatique des mises à jour de pilotes sur des terminaux pendant les mises à jour qualité.
Installer les mises à jour signées depuis des entités tierces	Autorisez l'installation de mises à jour issues d'entités tierces approuvées.
Limite de téléchargement des applications de l'opérateur mobile	Indiquez si vous souhaitez ignorer les limites de téléchargement d'opérateur mobile pour télécharger des applications et leurs mises à jour sur un réseau cellulaire.
Limite de téléchargement des mises à jour de l'opérateur mobile	Indiquez si vous souhaitez ignorer les limites de téléchargement d'opérateur mobile pour télécharger les mises à jour du système d'exploitation sur un réseau cellulaire.
Mises à jour approuvées par l'administrateur	
Demander l'approbation de la mise à jour	Activez l'obligation d'approbation avant le téléchargement des mises à jour sur le terminal. Activez cette option pour forcer les administrateurs à approuver explicitement les mises à jour avant leur téléchargement sur le terminal. Cette approbation s'effectue par l'intermédiaire de Groupes de mise à jour ou est individuelle, pour chaque mise à jour. Lorsque cette option est activée, vous devez accepter le CLUF requis pour le compte des utilisateurs avant que la mise à jour soit envoyée aux terminaux. Si un CLUF doit être accepté, une boîte de dialogue affiche le contrat. Pour approuver des mises à jour, naviguez vers **Cycle de vie > Mises à jour Windows**.
Optimisation de la distribution	
Mises à jour pair à pair	Autorise le téléchargement pair à pair de mises à jour.

2. Une fois que vous avez terminé la personnalisation du profil, n'oubliez pas de sélectionner **Enregistrer et publier** pour envoyer le profil sur vos terminaux.

Mises à jour des terminaux pour Windows Desktop

Workspace ONE UEM prend en charge la révision et l'approbation des mises à jour du système d'exploitation et OEM pour les terminaux Windows. La page **Mises à jour du terminal** répertorie

toutes les mises à jour disponibles pour les terminaux Windows enrôlés dans le groupe organisationnel sélectionné.

Application gérée sur le profil poste de travail Windows

Un administrateur peut gérer la suppression d'applications gérées sur les terminaux. Sous **Ajouter un nouveau profil de poste de travail Windows > Applications gérées**, l'administrateur peut activer ou désactiver la possibilité de conserver des applications gérées sur le terminal s'il est désenrôlé.

Navigation

Recherchez les **Mises à jour du terminal** disponibles dans **Ressources** > **Mises à jour du terminal**. Cette page répertorie les mises à jour **Windows** et les **Mises à jour OEM**.

Onglet Windows

Dans l'onglet **Windows**, vous pouvez approuver des mises à jour et les attribuer à des Smart Groups spécifiques, afin de répondre aux besoins de votre entreprise. Cet onglet affiche toutes les mises à jour accompagnées de leur date de publication, de leur plateforme, classification et groupe attribués. Seules les mises à jour disponibles pour les terminaux Windows enrôlés dans le groupe organisationnel sélectionné sont affichées. Si vous n'avez pas de terminal Windows enrôlé dans l'OG, aucune mise à jour ne s'affiche.

En sélectionnant le nom d'une publication, vous affichez une fenêtre contenant des informations détaillées, un lien vers la page de la base de connaissances Microsoft pour cette mise à jour, ainsi que l'état de son installation.

Ce processus nécessite la publication d'un profil Windows Update sur les terminaux avec le paramètre **Demander l'approbation de la mise à jour** activé.

Le statut d'installation de la mise à jour affiche le déploiement de la mise à jour au sein de vos terminaux. Consultez l'état du déploiement de la mise à jour en sélectionnant celle-ci dans la liste ou en sélectionnant **Afficher** dans la colonne État de l'installation.

État	Descriptions
Attribué	La mise à jour est approuvée et attribuée au terminal.
Approuvé	La mise à jour approuvée a bien été attribuée au terminal.
Disponible	La mise à jour est disponible pour installation sur le terminal.
Installation en attente	L'installation est approuvée et disponible mais pas encore installée.
Redémarrage en attente	L'installation est mise en pause jusqu'au redémarrage des terminaux.
Installé	La mise à jour a bien été installée.
Échec	La mise à jour n'a pas été installée.

Onglet des mises à jour OEM

À partir de cet onglet, vous pouvez voir toutes les mises à jour OEM déployées vers les terminaux Windows Desktop. Vous pouvez organiser l'affichage en liste par nom, niveau, type et catégorie de

terminal. Vous pouvez également filtrer les mises à jour affichées avec des filtres, y compris les pilotes audio, de pilotes de chipset, les mises à jour du BIOS et bien plus encore.

Pour afficher le statut d'installation du déploiement de la mise à jour, sélectionnez le nom de la mise à jour.

Utilisation des Lignes de base

Conservez vos terminaux Windows Desktop configurés conformément aux bonnes pratiques des lignes de base. Workspace ONE UEM combine les paramètres recommandés par l'industrie dans une configuration de ligne de base unique pour simplifier la sécurisation de vos terminaux. Les lignes de base réduisent le temps nécessaire à l'installation et à la configuration des terminaux Windows.

Micro-service Cloud

Les lignes de base utilisent un micro-service basé sur le cloud pour gérer le catalogue de stratégies. Si vous êtes un client sur site, assurez-vous que votre environnement peut communiquer avec le micro-service.

Les Lignes de base nécessitent une connectivité constante aux services du terminal

Tous les terminaux Windows enrôlés qui utilisent des lignes de base nécessitent une connectivité ininterrompue au serveur de services de terminal (DS) Workspace ONE UEM. Les terminaux ont besoin de cette connectivité constante pour que les états des lignes de base restent à jour.

Si vous utilisez une configuration de proxy ou certains paramètres de pare-feu, ces configurations peuvent interrompre la connexion entre vos terminaux Windows et le serveur DS. Par exemple, si des terminaux utilisent un VPN ou un réseau restreint pour accéder aux ressources, cette configuration interrompt la connexion au serveur DS. Sur ces terminaux, les Lignes de base risquent de ne pas être à jour.

Types de Lignes de base

- Personnalisé
  - Si vous disposez d'un fichier de sauvegarde d'objet de stratégie de groupe (GPO) existant, vous pouvez créer une ligne de base personnalisée avec ces stratégies. Utilisez le processus de modèle pour créer cette ligne de base personnalisée.
  - Vous pouvez également créer une ligne de base personnalisée sans modèle. Workspace ONE UEM propose des stratégies dans le processus **Créer la vôtre** pour les lignes de base.
- Évaluations CIS Windows : cette ligne de base applique les paramètres de configuration proposés par les évaluations CIS. Pour s'assurer que les Lignes de base n'utilisent que les meilleurs paramètres et configurations, le CIS (Center for Internet Security) certifie VMware pour fournir des favoris du secteur, tels que les évaluations CIS pour Windows.

- Ligne de base de sécurité Windows : cette ligne de base applique les paramètres de configuration proposés par Microsoft.

Les Lignes de base sont basées sur la version du système d'exploitation Windows de vos terminaux. Vous pourrez modifier la version du système d'exploitation de toute ligne de base ultérieurement. Pendant la configuration, vous pouvez choisir la ligne de base à utiliser et personnaliser les stratégies de base. Vous pouvez également ajouter des stratégies Microsoft ADMX supplémentaires dans le cadre du processus de configuration.

Considérations relatives à l'évaluation CIS

CIS signale les évaluations répertoriées pour établir une connexion plus sécurisée entre votre serveur et vos terminaux. Toutefois, ces évaluations ne sont actuellement pas prises en charge par le modèle de ligne de base d'évaluations CIS Windows. Les administrateurs doivent configurer ces évaluations. Pour plus d'informations, reportez-vous au rapport d'évaluation CIS Windows Server applicable.

- Configurez un titre et un texte d'ouverture de session interactif pour les utilisateurs qui tentent de se connecter.
- Installez l'extension AdmPwd GPO/CSE LAPS (Local Administrator Password Solution).

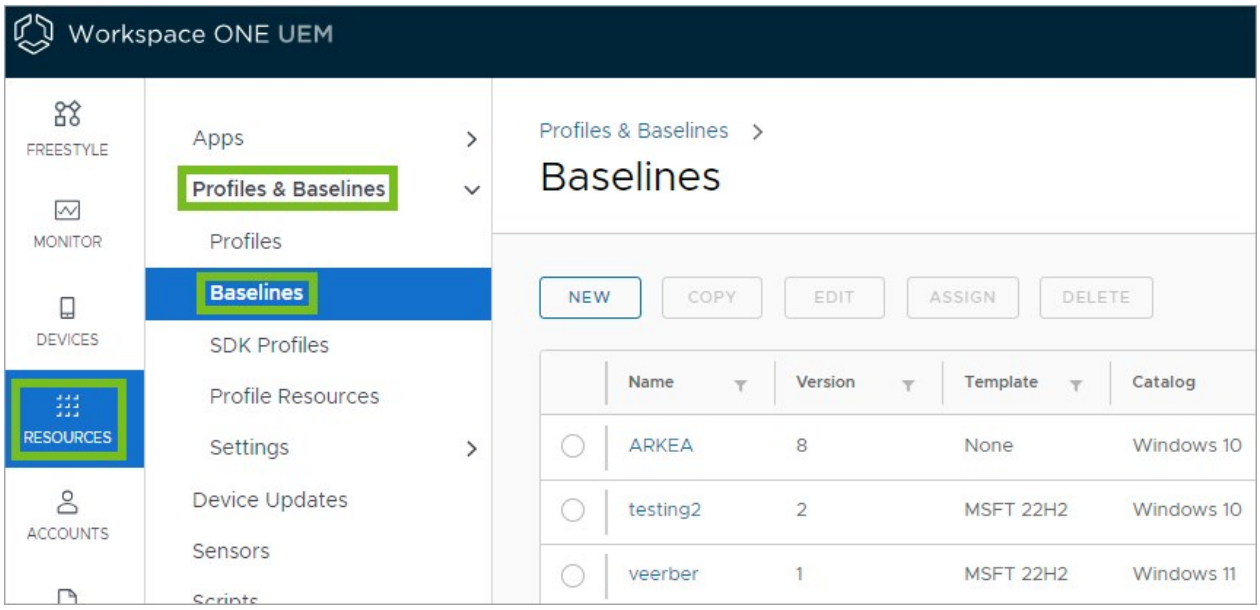
Attribution de lignes de base

Après avoir enrôlé un terminal dans Workspace ONE UEM, vous pouvez l'ajouter à un Smart Group et attribuer une ligne de base au groupe. Le terminal reçoit et applique l'ensemble des paramètres et configurations dans la ligne de base après le redémarrage du terminal. Le terminal vérifie les configurations de ligne de base lors de la publication de la ligne de base et selon les intervalles d'enregistrement définis. Lorsque vous transférez une ligne de base vers un terminal, Workspace ONE UEM stocke un snapshot des paramètres du terminal.

Vous pouvez limiter l'attribution de la ligne de base à l'aide de l'onglet **Exclusions** de la boîte de dialogue **Attribution**. Vous pouvez également choisir des Smart Groups à exclure de l'attribution.

Gestion des Lignes de base

Vous pouvez gérer vos lignes de base à partir de l'affichage en liste **Lignes de base**, disponible dans la console sous **Ressources > Profils et lignes de base > Lignes de base**.



À partir de cette page, vous pouvez modifier, copier et supprimer des lignes de base existantes.

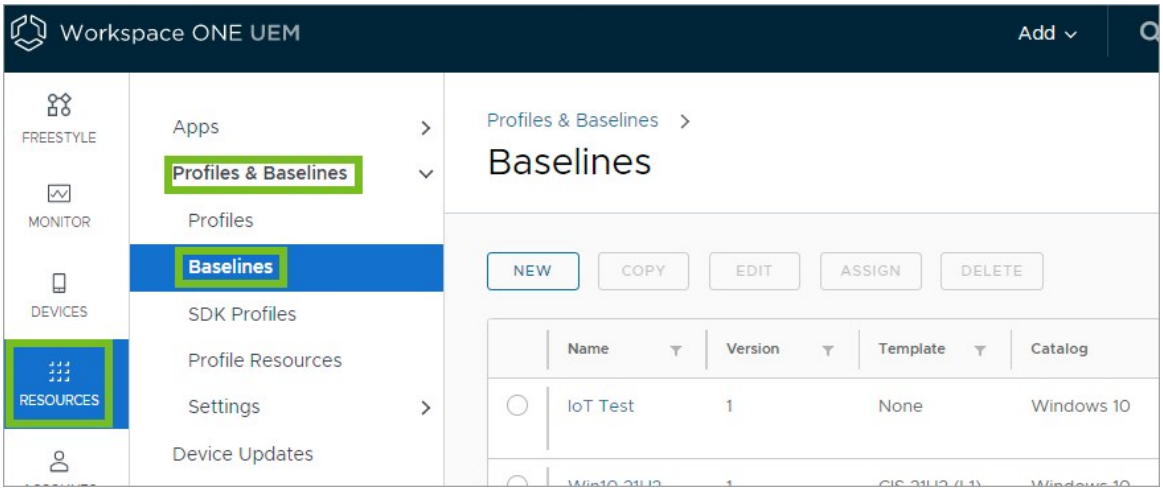
- **Copier** : vous pouvez copier des lignes de base et modifier plusieurs politiques dans les onglets **Personnaliser** et **Ajouter une politique** pour les adapter à un autre scénario de déploiement. Sélectionnez la ligne de base souhaitée pour afficher l'élément **Copier** du menu.
    - Le modèle de ligne de base ne peut pas être modifié. Si vous avez besoin d'un modèle différent, il vous faudra créer une nouvelle ligne de base.
    - Workspace ONE UEM enregistre la ligne de base copiée en tant que `Copy of <Baseline Name>`, mais vous pouvez tout de même modifier le nom.
    - Enregistrez la ligne de base copiée, mais n'attribuez pas de terminaux à celle-ci tant que vous n'avez pas modifié le champ **Géré par** (groupe organisationnel). Vous ne pouvez pas déplacer des lignes de base copiées pour lesquelles des terminaux sont déjà attribués.
    - Les groupes organisationnels (**Géré par**) et les lignes de base copiées ont des mises en garde.
        - Pour modifier le groupe organisationnel, modifiez la ligne de base copiée après l'avoir enregistrée.
        - Vous pouvez déplacer la ligne de base copiée vers les groupes d'organisation enfants ou la laisser dans le groupe d'organisation d'origine.
        - En revanche, vous ne pouvez pas déplacer la ligne de base copiée plus haut dans la hiérarchie du groupe d'organisation. Il s'agit d'un comportement similaire à celui des profils.
- **Supprimer** : Si vous supprimez une ligne de base qui a été transférée vers des terminaux, les paramètres du terminal reviennent aux paramètres précédents en fonction du snapshot stocké par Workspace ONE UEM.

Vous pouvez voir quelles lignes de base sont appliquées à un terminal sur la page **Détails du terminal**.

Exemple de copie d'une ligne de base

Voici comment copier une ligne de base existante et mettre à jour le champ **Géré par** pour déplacer la ligne de base vers un sous-groupe organisationnel.

1. Dans Workspace ONE UEM Console, accédez au groupe organisationnel applicable.
2. Accédez à **Ressources > Profils et lignes de base > Lignes de base**.



3. Sélectionnez une ligne de base dans la liste et sélectionnez **Copier**.
4. Mettez à jour le nom de la ligne de base dans le champ **Nom de la ligne de base**. Vous ne pouvez pas mettre à jour le groupe organisationnel pour le moment.
5. Parcourez l'assistant Lignes de base pour effectuer des mises à jour si nécessaire. Vous n'avez pas à apporter de modifications. Vous pouvez sélectionner **Suivant** pour n'importe quel onglet.
6. Dans l'onglet **Résumé**, cliquez sur **Enregistrer et attribuer**.
7. Sur la page **Attribuer une ligne de base**, cliquez sur **Analyse**. Cette action annule l'attribution de terminaux à la ligne de base copiée.
   Important : n'attribuez pas de terminaux à votre ligne de base copiée tant que vous n'avez pas modifié le groupe organisationnel.
8. Sélectionnez la ligne de base copiée dans la liste et cliquez sur **Modifier**.
9. Mettez à jour le groupe organisationnel en sélectionnant un sous-groupe organisationnel dans **Général > Géré par**.
10. Parcourez l'assistant et cliquez sur **Enregistrer et publier**.
11. Sélectionnez la ligne de base copiée et cliquez sur **Attribuer** lorsque vous êtes prêt à ajouter des terminaux.

Réappliquer des lignes de base

Il existe plusieurs façons d'activer l'application locale des lignes de base. Pour exécuter un script qui ajoute la clé de registre à réappliquer sur un terminal, vous pouvez utiliser des capteurs, un provisionnement de produit, des scripts dans applications et livres, ou créer un profil de paramètres personnalisés. Pour plus d'informations sur l'implémentation de ceci et/ou sur la gestion des lignes de base et des stratégies de groupe, reportez-vous à : Zone technique : Gestion des lignes de base

avec des stratégies de groupe.

État de conformité des Lignes de base

Vérifiez que votre terminal respecte les lignes de base à l'aide de l'état de conformité de la ligne de base. Recherchez l'**État de la conformité** dans la console sous **Ressources > Profils et lignes de base > Lignes de base**, sélectionnez la ligne de base et consultez la fiche **État de conformité**. La fiche **État de conformité de la ligne de base** indique quand les terminaux sont conformes, intermédiaires, non conformes ou non disponibles.

Remarque : L'état de conformité de la ligne de base s'applique uniquement aux lignes de base créées à partir de l'interface utilisateur. Vous ne pouvez pas voir l'état de conformité des lignes de base personnalisées créées à l'aide de fichiers de sauvegarde GPO.

- L'état **Intermédiaire** identifie les terminaux de 85 à 99 % conformes. Cet état est un indicateur que la conformité de vos terminaux a été réduite avec les lignes de base attribuées.
- L'état **Non disponible** signifie que Workspace ONE UEM Console n'a pas d'échantillon de conformité pour le terminal. Vous pouvez forcer un échantillon en ouvrant simplement la ligne de base et en la publiant de nouveau.

Interrogation des états de conformité des lignes de base

Vous pouvez interroger les terminaux pour obtenir des échantillons de lignes de base afin d'actualiser l'état de conformité. Pour interroger une ligne de base, commencez par la vue **Détails du terminal**.

Remarque : Vous pouvez interroger l'état de conformité d'un terminal spécifique mais pas de plusieurs terminaux à la fois.

1. Dans Workspace ONE UEM console, accédez à **Terminaux** et sélectionnez le terminal Windows Desktop spécifique dans l'**Affichage en liste des terminaux**.
2. Sélectionnez **Plus d'actions > Requête > Lignes de base**. Ce processus initie la commande de requête.
3. Pour afficher l'état de conformité mis à jour de la ligne de base, accédez à **Ressources > Profils et lignes de base > Lignes de base**, sélectionnez la ligne de base et consultez la fiche **État de conformité**.

Vérification de l'état de conformité

Si un paramètre sur le terminal ne correspond pas à la ligne de base, utilisez l'onglet Dépannage dans **Détails du terminal** pour vérifier que Workspace ONE UEM a reçu l'échantillon du terminal.

1. Dans Workspace ONE UEM console, accédez à **Terminaux** et sélectionnez le terminal Windows Desktop spécifique.
2. Sélectionnez l'onglet **Dépannage** dans la vue **Détails du terminal** pour afficher le **Journal des événements** et l'onglet **Commandes**.
3. Dans l'onglet **Commandes**, reportez-vous à la liste des commandes de requête de ligne de base. Vous pouvez voir les états répertoriés.
    - **Mise en file d'attente :** le système a entré la commande dans la base de données

du serveur.

- **En attente** : Le terminal a reçu la demande mais n'a pas répondu.
- **Traité** : Le terminal a envoyé un échantillon ou l'échantillon est mis en file d'attente pour la prochaine session utilisateur.

4. Dans l'onglet **Journal des événements**, recherchez un **Événement** qui confirme **Réponse d'échantillon de ligne de base reçue**.

Création d'une ligne de base

Créez une ligne de base avec ou sans modèle pour configurer vos terminaux conformément aux paramètres et configurations recommandés par l'industrie. Workspace ONE UEM organise les lignes de base en fonction des favoris du secteur, y compris les évaluations du CIS et les lignes de base de sécurité Windows de Microsoft.

Conditions prérequises

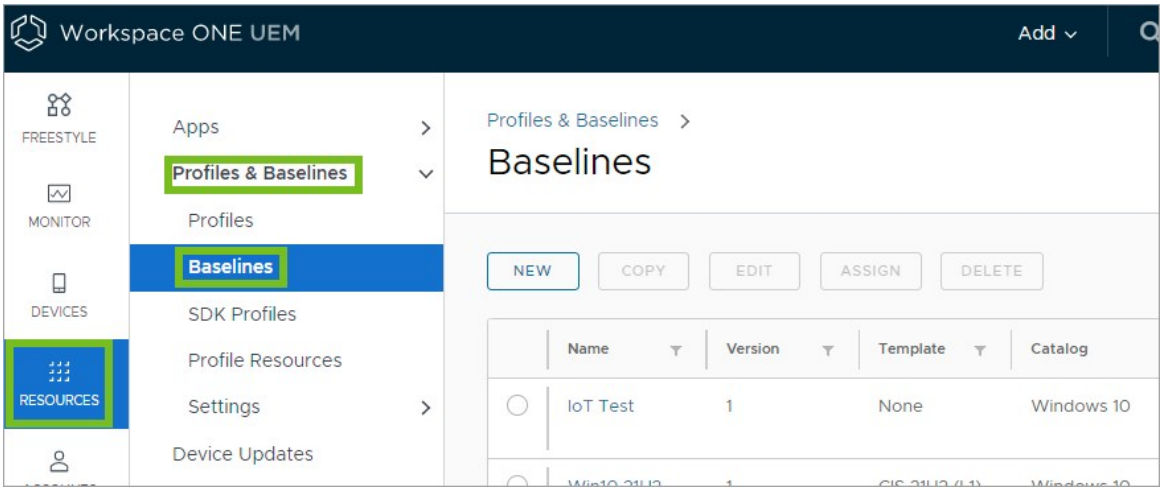
Vos terminaux doivent être enrôlés dans Workspace ONE UEM et Workspace ONE Intelligent Hub doit être installé.

Si vous publiez une ligne de base personnalisée en utilisant un fichier de sauvegarde GPO, vous devez ajouter le fichier LGPO.exe à tous les terminaux auxquels vous souhaitez attribuer une ligne de base. Vous devez installer le fichier EXE sur `C:\ProgramData\Airwatch\LGPO\LGPO.exe`. Si vous utilisez le modèle d'évaluation CIS, le modèle de sécurité Windows ou l'assistant Créer la vôtre, vous n'avez pas besoin d'ajouter ce fichier.

Création de lignes de base avec un modèle

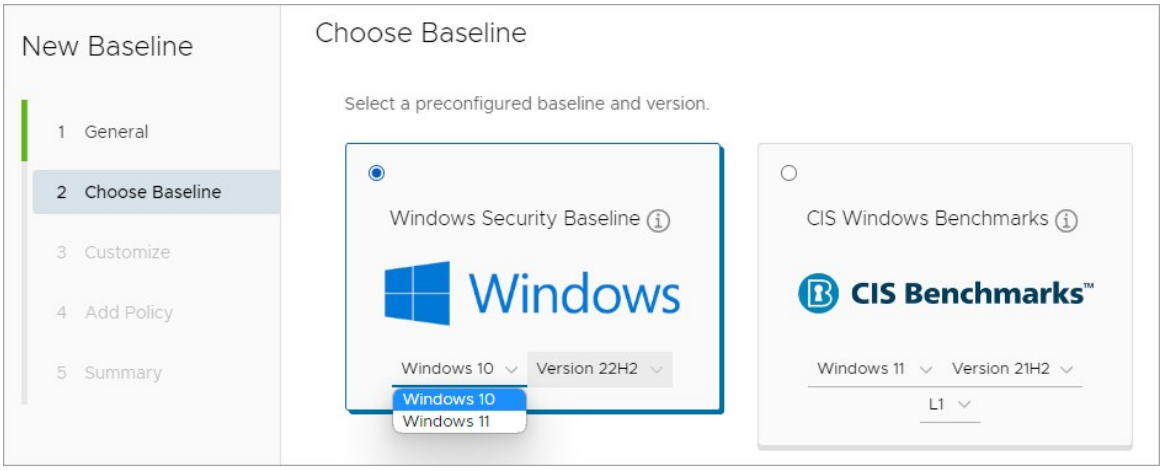
Si vous souhaitez utiliser un fichier de sauvegarde GPO pour créer vos lignes de base, utilisez un modèle.

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



2. Sélectionner **Utiliser un modèle**.
3. Entrez un **Nom de ligne de base**, une **Description** et sélectionnez le Smart Group par lequel la ligne de base est **gérée**. Sélectionnez ensuite **Suivant**.

4. Sélectionnez une ligne de base.



Paramètre	Description
Ligne de base de sécurité Windows	Cette ligne de base applique les paramètres de configuration proposés par Microsoft. Sélectionnez la plateforme et la version du système d'exploitation à appliquer.
Évaluations CIS Windows	Cette ligne de base applique les paramètres de configuration proposés par les évaluations CIS. Sélectionnez la plateforme du système d'exploitation, la version et le niveau d'évaluation à appliquer.
Ligne de base personnalisée	Téléchargez un fichier ZIP avec une sauvegarde GPO. Vous devez créer cette ligne de base à l'extérieur de Workspace ONE UEM. La sauvegarde doit être inférieure à 5 Mo et contenir au moins un dossier GPO.

5. Sélectionnez **Suivant**.
6. Personnalisez la ligne de base en fonction des besoins. Vous pouvez modifier n'importe quelle stratégie ADMX existante configurée dans la ligne de base. Lorsque vous créez une ligne de base personnalisée à partir d'une ligne de base GPO, vous ne pouvez pas personnaliser les stratégies ADMX existantes.

   Veillez à utiliser des SID lors de la création de stratégies ADMX de droits d'utilisateur. Pour plus d'informations, reportez-vous à Identificateurs de sécurité connus dans les systèmes d'exploitation Windows.
7. Sélectionnez **Suivant**.
8. Ajoutez des stratégies supplémentaires à la ligne de base. Ces stratégies proviennent de fichiers Microsoft ADMX. Recherchez une stratégie à ajouter et configurez-la.
9. Sélectionnez **Suivant**.
10. Examinez le résumé et sélectionnez **Enregistrer et attribuer**. Le résumé inclut toutes les stratégies personnalisées ou ajoutées.
11. Lors de l'attribution, entrez le Smart Group contenant les terminaux Windows auxquels vous souhaitez attribuer la ligne de base. Vous pouvez redéfinir quels terminaux obtiennent la ligne de base à l'aide de l'onglet **Exclusions**. Entrez les Smart Groups que vous souhaitez exclure de l'attribution.
    Les exclusions remplacent les attributions. Si un terminal se trouve dans un Smart Group

exclu, ce terminal ne reçoit pas la ligne de base. Si ce terminal disposait déjà de la ligne de base issue d'une attribution précédente, la ligne de base est supprimée du terminal.

12. Redémarrez les terminaux pour déployer des lignes de base.

Création de lignes de base personnalisées

Si vous ne souhaitez pas utiliser un modèle pour créer vos lignes de base, suivez ces étapes pour créer la vôtre.

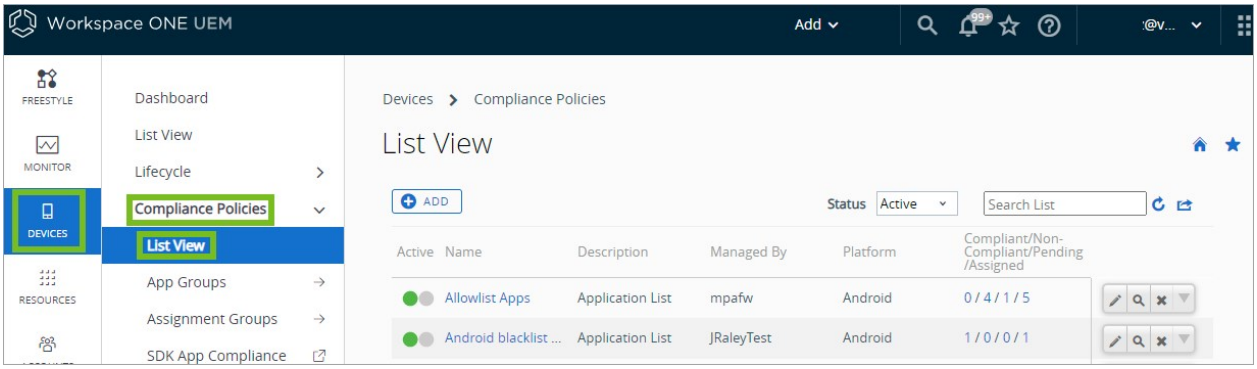
1. Accédez à **Ressources** > **Profils et lignes de base** > **Lignes de base** et sélectionnez **Nouveau**.
2. Sélectionnez **Créer la vôtre**.
3. Entrez un **Nom de ligne de base**, une **Description** et sélectionnez le Smart Group par lequel la ligne de base est **gérée**. Sélectionnez ensuite **Suivant**.
4. Dans la fenêtre **Ajouter une stratégie**, sélectionnez la version du système d'exploitation Windows, puis commencez à entrer un nom de stratégie.
   Par exemple, entrez `User` ou `Computer Configuration`, puis sélectionnez la stratégie souhaitée dans la liste.
5. Ajoutez des stratégies supplémentaires à la ligne de base.
   Ces stratégies proviennent de fichiers Microsoft ADMX. Recherchez une stratégie à ajouter et configurez-la. Ces stratégies sont les mêmes que celles disponibles avec les modèles, mais elles s'affichent comme **Non configurées**. Vous devez activer et configurer la stratégie ou la désactiver.
6. Sélectionnez l'état **Activée**, **Désactivée** ou **Non configurée** pour la stratégie sur les terminaux.
7. Examinez le résumé et sélectionnez **Enregistrer et attribuer**. Le résumé inclut toutes les stratégies.
8. Lors de l'attribution, entrez le Smart Group contenant les terminaux Windows auxquels vous souhaitez attribuer la ligne de base. Vous pouvez redéfinir quels terminaux obtiennent la ligne de base à l'aide de l'onglet **Exclusions**. Entrez les Smart Groups que vous souhaitez exclure de l'attribution.
   Les exclusions remplacent les attributions. Si un terminal se trouve dans un Smart Group exclu, ce terminal ne reçoit pas la ligne de base. Si ce terminal disposait déjà de la ligne de base issue d'une attribution précédente, la ligne de base est supprimée du terminal.
9. Redémarrez les terminaux pour déployer des lignes de base.

politiques de conformité

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

Stratégies de conformité dans Workspace ONE UEM

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



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

Dell BIOS Verification pour Workspace ONE UEM

Utilisez Dell Trusted Device (anciennement Dell BIOS Verification) pour préserver la sécurité de vos terminaux Dell Windows Desktop. Ce service analyse le BIOS de vos terminaux Dell et envoie un rapport d'état à Workspace ONE UEM pour vous permettre d'intervenir sur n'importe quel terminal compromis.

Avantages de Dell Trusted Device

Le BIOS joue un rôle dans la gestion de la santé et de la sécurité globales d'un terminal. Les

systèmes informatiques modernes utilisent le microprogramme BIOS pour initialiser le matériel pendant le processus de démarrage ainsi que pour les services d'exécution qui prennent en charge le système d'exploitation et les applications. Du fait de cette place privilégiée dans l'architecture de terminaux, le fait de modifier le microprogramme BIOS sans les autorisations requises constitue une menace significative. Le service Dell Trusted Device assure une validation du BIOS sécurisée grâce à un modèle de réponse signée sécurisé. L'état de la validation sécurisée vous permet d'agir sur les terminaux compromis à l'aide du moteur de stratégie de conformité.

Préparer vos terminaux à Dell Trusted Device

Pour utiliser Dell Trusted Device sur vos terminaux Windows Desktop, vous devez d'abord l'installer sur les terminaux en question. Vous devez télécharger le client le plus récent auprès de Dell (https://www.dell.com/support/home/product-support/product/trusted-device/drivers). Vous pouvez utiliser Software Distribution pour installer le client sur vos terminaux Dell Windows Desktop.

États de Dell BIOS Verification

Après avoir installé le client sur vos terminaux, vous pouvez consulter le rapport d'état sur la page Détails du terminal. Il existe différents états :

- Réussite : le client Dell Trusted Device est installé sur le terminal et le terminal est sécurisé.
- Échec : le client Dell Trusted Device est installé et a détecté l'un des problèmes suivants :
    - L'événement Prévérification renvoie un résultat d'échec. Ce résultat se produit lorsque le client détecte une signature binaire non valide.
    - L'événement Utilitaire du BIOS renvoie un résultat d'échec pour le test de validation.
    - L'événement Traitement du serveur BIOS renvoie un résultat d'échec en raison d'une signature non valide, d'un code de sortie non valide ou d'un problème de synchronisation de l'état de la charge utile.
- Avertissement : le service Dell Trusted Device est installé et le client détecte un problème. Le terminal n'est peut-être pas sécurisé ; examinez le problème. Un état d'avertissement peut avoir plusieurs causes, répertoriées dans la liste suivante.
    - Absence de connexion réseau
    - Argument de ligne de commande non valide
    - Application exécutée avec des privilèges insuffisants
    - Erreurs internes du client
    - Erreur renvoyée par le serveur
    - Problèmes de pilote au niveau du client
    - Résultats inconnus dans la vérification du BIOS
- Une icône d'avertissement grisée signifie que le client Dell Trusted Device n'est pas installé sur le terminal.

Détection des terminaux compromis avec attestation d'intégrité

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.

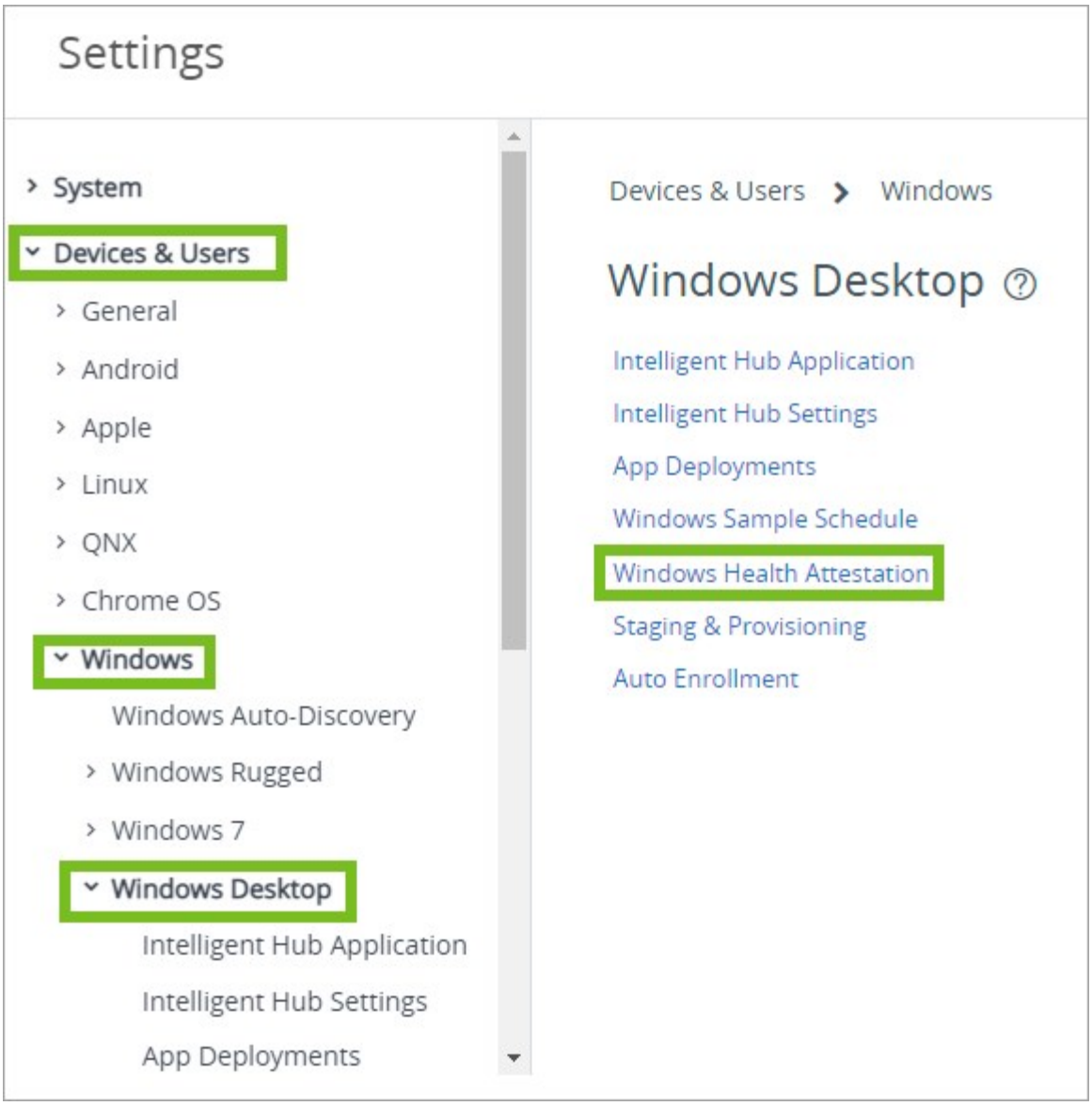
Workspace ONE UEM vous permet de configurer le service d'attestation d'intégrité de Windows pour garantir la conformité des terminaux. Si l'une des vérifications activées échoue, le moteur de politique de conformité de Workspace ONE UEM applique les mesures de sécurité en fonction de la politique de 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.

Paramètres	Descriptions
Démarrage sécurisé désactivé	Activez ce paramètre pour signaler un état du 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.
Stratégie de prévention de l'exécution des données (DEP) désactivée	Activez ce paramètre pour signaler un état du terminal compromis lorsque la stratégie 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 état 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 état du 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.
Protection contre les programmes malveillants à lancement anticipé désactivée	Activez ce paramètre pour signaler un état du 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.

Paramètres	Descriptions
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**.

Applications Windows Desktop

Vous pouvez utiliser les applications Workspace ONE UEM en plus des fonctionnalités Workspace ONE UEM MDM pour renforcer la sécurité des terminaux et leur ajouter des fonctions supplémentaires. Utilisez Workspace ONE Intelligent Hub pour Windows pour cataloguer et gérer vos applications et pour faciliter la communication entre le terminal et Workspace ONE UEM Console.

Applications de productivité Workspace ONE

Utilisez Workspace ONE Content pour protéger le contenu d'entreprise sur les terminaux mobiles. Déployez Workspace ONE Web pour activer la navigation Web sécurisée pour vos utilisateurs finaux. Téléchargez Workspace ONE Intelligent Hub pour Windows pour surveiller vos terminaux de manière plus granulaire.

Déployer des applications Win32 sur des terminaux Windows Desktop nécessite la présence de Workspace ONE Intelligent Hub sur le terminal.

Important : toutes les applications publiques déployées sur des terminaux Windows Desktop sont des applications non gérées. Les applications non gérées ne peuvent ni être chargées sur des terminaux (les utilisateurs doivent les télécharger eux-mêmes), ni être supprimées des terminaux par le biais de la fonction d'effacement des données d'entreprise.

Application VMware Workspace ONE pour Windows Desktop

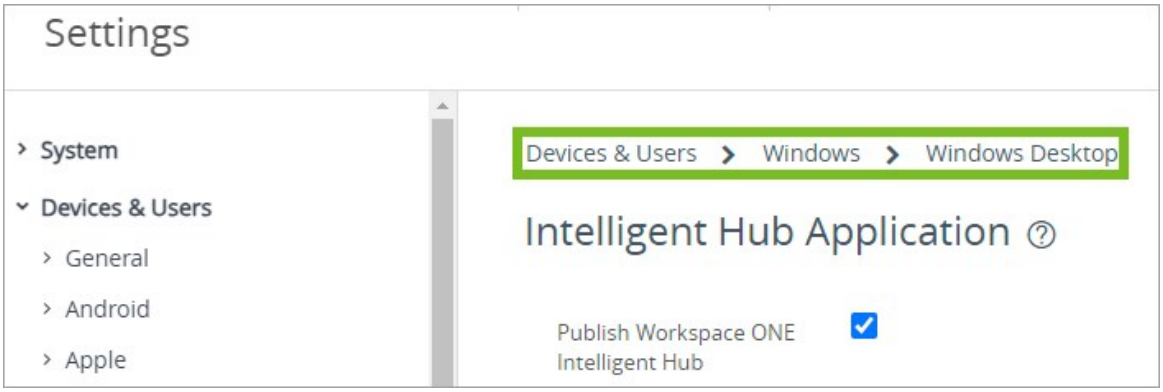
Lorsque l'application Workspace ONE est installée sur des terminaux, les utilisateurs peuvent se connecter à Workspace ONE afin d'accéder à un catalogue d'applications activé par votre organisation. Une fois l'application configurée à l'aide d'une authentification Single Sign-On, les utilisateurs n'ont plus besoin d'entrer leurs informations d'identification de connexion au démarrage de l'application.

L'interface utilisateur Workspace ONE fonctionne de la même manière sur les téléphones, tablettes et ordinateurs de bureau. Workspace ONE ouvre une page du Launcher qui affiche des ressources déployées vers Workspace ONE. Les utilisateurs peuvent toucher ou cliquer pour rechercher, ajouter et mettre à jour des applications, effectuer un clic droit sur une application pour la supprimer de la page et aller sur la page du catalogue pour ajouter des ressources autorisées. Si une application nécessite l'enrôlement d'un terminal, Workspace ONE utilise la gestion évolutive pour lancer le processus d'enrôlement pour l'utilisateur.

Configurer Workspace ONE Intelligent Hub pour Windows Desktop

Vous pouvez mettre à jour les paramètres de Workspace ONE Intelligent Hub pour répondre à certains besoins de votre entreprise.

1. Accédez à **Groupes et paramètres** > **Tous les paramètres** > **Terminaux et utilisateurs** > **Windows** > **Windows Desktop** > **Paramètres Intelligent Hub**.



2. Configurez l'élément de menu **Intervalle d'échantillonnage des données (min)** pour définir les intervalles pendant lesquels Workspace ONE Intelligent Hub prend des échantillons de données.
3. Configurez l'élément de menu **Sécurité des canaux MDM** pour définir la sécurité de la couche d'application entre le terminal et Workspace ONE UEM Console.
4. Configurez les paramètres de **Confidentialité** si vous utilisez des outils d'analyse pour la collecte de données.
    - **Afficher l'écran de confidentialité** : affichez un écran pour demander à vos utilisateurs de collecter des données.
    - **Collecter les analyses** : collectez divers points de données, tels que les incidents d'application et les numéros de point de terminaison, et envoyez ces données à votre fournisseur d'analyse d'applications.

Étapes suivantes

Vous pouvez empêcher les utilisateurs finaux de désactiver le service Workspace ONE UEM sur leurs terminaux à l'aide d'un profil de paramètres personnalisés.

Ajout d'applications Win32 et gestion

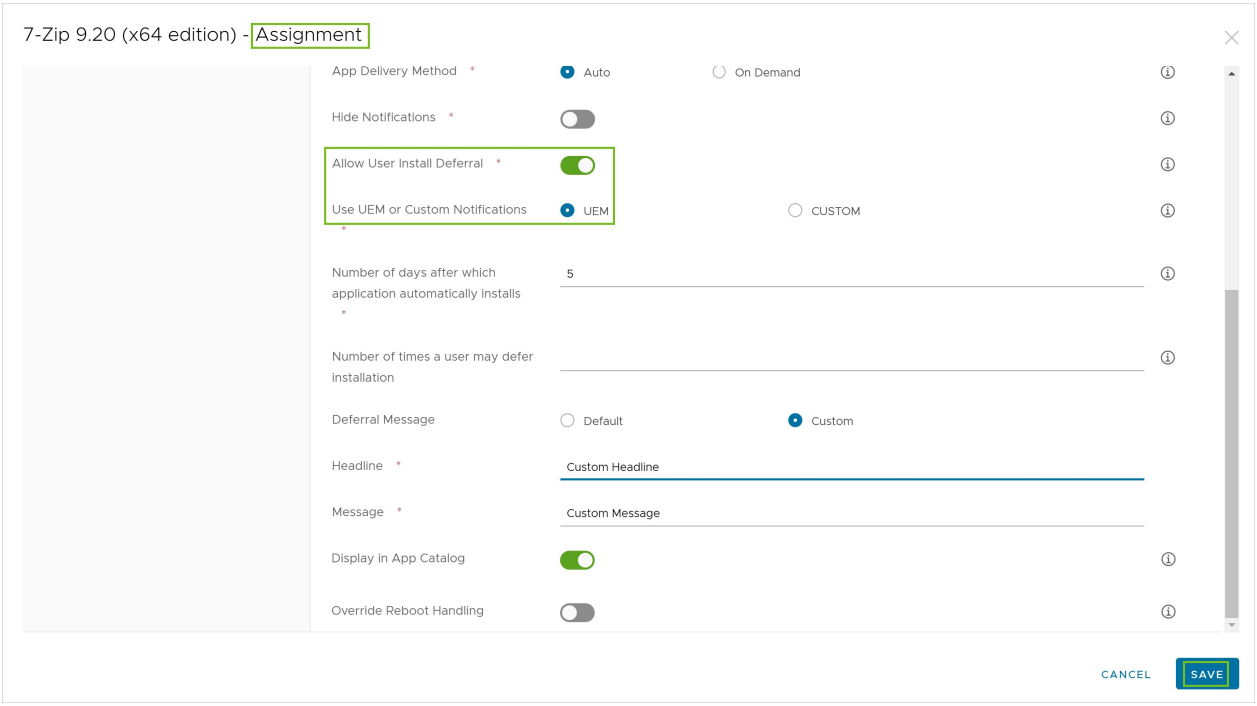
Lors de l'installation d'une nouvelle application Win32, vous démarrez dans la Workspace ONE UEM Console, sous **Ressources > Applications > Natives > Ajouter > Fichier d'application**. Vous pouvez choisir le fichier dans Fichier local ou Lien, puis cliquer sur **Enregistrer**. Une fois l'application choisie, vous verrez une fenêtre **Ajouter une application** s'ouvrir, qui vous permet de définir et de personnaliser les paramètres.

Pour plus d'informations sur le déploiement d'applications Win32 traditionnelles sur des terminaux Windows, consultez cet article Tech Zone.

Différer l'installation de l'application dans UEM

En tant qu'administrateur, vous pouvez activer l'option permettant aux utilisateurs de gérer et de différer l'installation de l'application. Dans le menu **Attribution** d'application, sous **Distribution**, activez l'option **Autoriser le report d'installation par l'utilisateur**. Ensuite, sous **Utiliser les**

notifications UEM ou personnalisées, choisissez **UEM**. Vous pouvez désormais définir la durée pendant laquelle l'utilisateur final peut reporter l'installation de l'application.



Vous pouvez choisir de définir : 1. Le Délai de report : nombre de **jours** après lesquels l'application s'installe automatiquement. 1. Le Nombre de reports : nombre de **fois** qu'un utilisateur peut reporter l'installation. 1. Délai de report et nombre de reports.

Si vous choisissez de définir les deux options, la première chronologie d'option de report atteinte sera le moment où elle entrera en vigueur. À ce stade, l'utilisateur aura la possibilité de différer une dernière fois, mais seulement pendant 30 minutes. Ensuite, l'application démarre le processus d'installation. *Exemple : L'administrateur définit le délai de report sur 10 jours et définit le nombre de reports sur 3. L'événement qui se produit en premier sera celui qui s'applique. Par conséquent, si l'utilisateur atteint cette 3e option de nombre reports dans 4 jours, l'utilisateur verra l'option de report pendant seulement 30 minutes, puis l'application démarrera l'installation.*

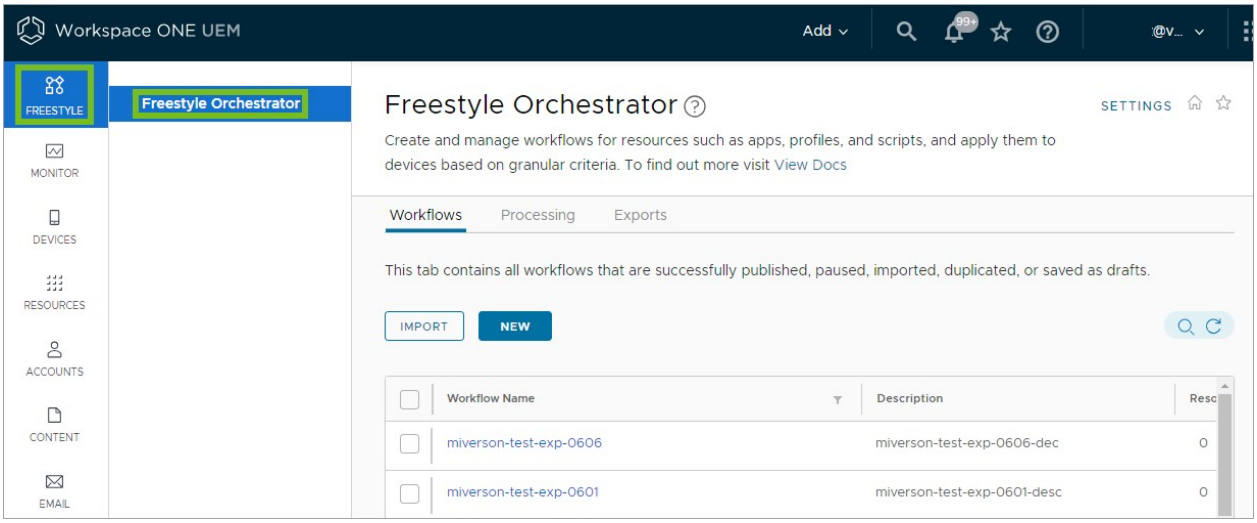
L'UEM propose un message de notification d'alerte de report par défaut. Cependant, si vous souhaitez créer votre propre message, sous **Message par défaut**, choisissez **Personnalisé** et fournissez vos propres **En-tête** et **Message** de report.

Collecter des données avec des Capteurs pour les terminaux Windows Desktop

Les terminaux Windows Desktop contiennent de nombreux attributs tels que le matériel, le système d'exploitation, les certificats, les correctifs, les applications et bien plus encore. Avec les Capteurs, vous pouvez collecter des données pour ces attributs à l'aide de Workspace ONE UEM Console. Affichez les données dans Workspace ONE Intelligence et dans Workspace ONE UEM.

Fonctionnalité Freestyle

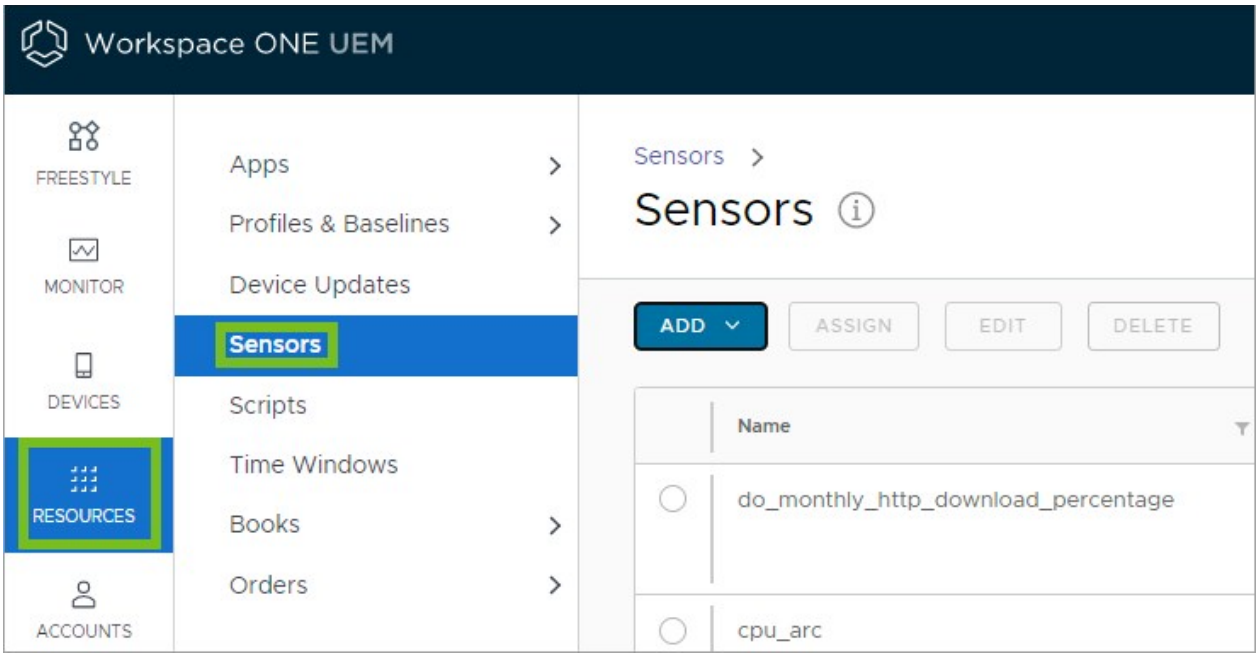
Capteurs est une fonctionnalité Freestyle disponible pour les environnements SaaS. Pour plus d'informations sur Freestyle, accédez à Freestyle Orchestrator.



Description des Capteurs

Un très grand nombre d'attributs sont associés aux terminaux. Ce nombre augmente lorsque vous effectuez le suivi de différentes applications, versions du système d'exploitation, correctifs et autres variables en constante évolution. Il peut être difficile d'effectuer le suivi de tous ces attributs.

Workspace ONE UEM effectue le suivi d'un nombre limité d'attributs de terminaux par défaut. Toutefois, avec des Capteurs, vous pouvez effectuer le suivi d'attributs de terminaux spécifiques. Par exemple, vous pouvez créer un capteur qui effectue le suivi des détails de pilote pour un pilote de souris, les informations de garantie du système d'exploitation et la valeur de registre de vos applications internes. Les Capteurs vous permettent d'effectuer le suivi de divers attributs sur vos terminaux. Recherchez des **Capteurs** dans la page de navigation principale de Workspace ONE UEM Console sous **Ressources**.



Pour utiliser les données de capteurs depuis Workspace ONE UEM, vous pouvez utiliser Workspace ONE Intelligence. Workspace ONE Intelligence dispose de tableaux de bord et de rapports dans lesquels vous pouvez afficher et analyser vos données de capteurs. Le transfert de données entre les deux systèmes s'effectue via le protocole HTTP sécurisé à l'aide de SSL sur le port 443.

Important : Les Capteurs ne sont pas autorisés à être attribués à des terminaux personnels pour des raisons de confidentialité.

Options Workspace ONE UEM

Déclencheurs de capteurs

Lors de la configuration des capteurs, vous pouvez contrôler le moment où le terminal signale les données du capteur à Workspace ONE UEM console avec des déclencheurs. Vous pouvez planifier ces déclencheurs en fonction de la planification de l'échantillon de Windows ou d'événements spécifiques du terminal, tels que la connexion et la déconnexion.

Ajout de scripts PowerShell

Le script PowerShell que vous créez détermine la valeur de chaque capteur.

Détails du terminal > Capteurs

Vous pouvez afficher les données d'un terminal dans l'onglet **Capteurs** de la page **Détails du terminal**.

Le paramètre de configuration **État du terminal** doit être activé dans votre centre de données pour que Workspace ONE UEM puisse afficher les données des Capteurs des terminaux dans l'onglet **Capteurs**. Workspace ONE UEM active cette configuration pour les clients SaaS.

Remarque : Workspace ONE UEM travaille sur une solution pour les environnements sur site, mais tant que cette solution n'est pas créée, l'onglet **Capteurs** n'est pas disponible sur la page **Détails du terminal** pour les déploiements sur site.

Options Workspace ONE Intelligence

Rapports et tableaux de bord pour analyser les données

Si vous utilisez le service Workspace ONE Intelligence, vous pouvez exécuter un rapport ou créer un tableau de bord pour afficher les données de vos Capteurs et interagir avec ces dernières. Lorsque vous exécutez des rapports, utilisez la catégorie **Workspace ONE UEM**, **Capteurs du terminal**. Vous pouvez rechercher vos capteurs et les sélectionner pour des requêtes dans les rapports et les tableaux de bord.

RBAC pour contrôler l'accès aux données

Pour contrôler qui a accès aux capteurs, utilisez la fonctionnalité de contrôle d'accès basé sur les rôles (RBAC, Roles Based Access Control) dans Workspace ONE Intelligence. RBAC attribue des autorisations à des administrateurs. Utilisez-les pour empêcher ou autoriser des utilisateurs spécifiques de Workspace ONE Intelligence à accéder aux données des capteurs.

Chiffrement

Toutes les données inactives sont chiffrées dans Workspace ONE Intelligence. Pour plus d'informations, consultez le contenu dans VMware Cloud Trust Center. Ce site fournit des rapports détaillés sur les certificats de conformité, sur CAIQ, SOC2 et SOC3, et donne d'autres meilleures pratiques en matière de sécurité.

Utiliser Write-Ouput et Not Write-Host dans les scripts

La chaîne `Write-Host` d'un script écrit directement sur l'écran et ne signale pas la sortie du capteur à Workspace ONE Intelligence. Cependant, la chaîne `Write-Output` écrit dans le pipeline, utilisez-la plutôt que `Write-Host`. Mettez à jour les scripts applicables vers `Write-Output` ou `echo` (`echo` est un alias pour `Write-Output`.)

Pour plus d'informations, accédez aux rubriques dans Microsoft | Docs pour Write-Host et Write-Output.

Exemple de script non opérationnel

- Fuseau horaire du retour
- Type de retour : Chaîne

```
$os=Get-TimeZone
write-host $os
```

- Write-Host n'est pas la sortie du script, il n'y a donc aucune sortie du script.
- Write-Host écrit directement dans l'« écran » et non dans le pipeline.

Exemple de script opérationnel

- Fuseau horaire du retour

- Type de retour : Chaîne

```
$os=Get-TimeZone
write-output $os
```

Documentation de Workspace ONE Intelligence

Pour plus d'informations sur le travail dans Workspace ONE Intelligence, accédez à Produits VMware Workspace ONE Intelligence.

Terminaux Windows Desktop et données des capteurs

Les données des capteurs ne sont pas stockées localement sur les terminaux Windows. Un capteur exécute un code PowerShell qui évalue un attribut sur un système et transmet ces données à Workspace ONE Intelligence. Après l'évaluation et la transmission, le processus PowerShell s'arrête.

Exemples de scripts PowerShell pour les Capteurs

Lorsque vous créez des Capteurs pour les terminaux Windows, vous devez charger un script PowerShell ou entrer les commandes PowerShell dans la zone de texte proposée lors de la configuration dans Workspace ONE UEM Console. Ces commandes renvoient les valeurs des attributs du capteur.

Les exemples suivants contiennent les paramètres et le code requis. Vous pouvez également consulter le site https://code.vmware.com/samples ?id=4930 pour voir d'autres exemples de Capteurs.

Remarque : Tout capteur qui renvoie une valeur de type de données date-heure utilise le format ISO.

Vérifier le niveau de batterie restant

- **Type de valeur** : Entier
- **Contexte d'exécution** : Utilisateur

```
$battery_remain=(Get-WmiObject win32_battery).estimatedChargeRemaining |
Measure-Object -Average | Select-Object -ExpandProperty Averageecho $battery_re
main
```

Obtention du numéro de série

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$os=Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycontin
ue
echo $os.SerialNumber
```

Obtention de la date système

- **Type de valeur** : DateTime
- **Contexte d'exécution** : Utilisateur

```
$date_current = get-Date -format s -DisplayHint Date
echo $date_current
```

Vérification de l'activation du TPM

- **Type de valeur** : Booléen(ne)
- **Contexte d'exécution** : Administrateur

```
$obj = get-tpm
echo $obj.TpmReady
```

Vérification du verrouillage du TPM

- **Type de valeur** : Booléen(ne)
- **Contexte d'exécution** : Administrateur

```
$obj = get-tpm
echo $obj.LockedOut
```

Obtention de l'heure de correction du TPM verrouillé

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Administrateur

```
$tpm=get-tpm
echo $tpm.LockoutHealTime
```

Vérification de la présence du SMBIOS

- **Type de valeur** : Booléen(ne)
- **Contexte d'exécution** : Utilisateur

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycont
inue
echo $os.SMBIOSPresent
```

Vérification de la version BIOS de SMBIOS

- **Type de valeur** : Booléen(ne)
- **Contexte d'exécution** : Utilisateur

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycont
inue
echo $os.SMBIOSBIOSVersion
```

Affichage de la version du BIOS

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycont
inue
echo $os.Version
```

Affichage de l'état du BIOS

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$os = Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycont
inue
echo $os.Status
```

Affichage de l'utilisation moyenne du CPU (%)

- **Type de valeur** : Nombre entier
- **Contexte d'exécution** : Utilisateur

```
$cpu_usage= Get-WmiObject win32_processor | Select-Object -ExpandProperty LoadP
ercentage
echo $cpu_usage
```

Affichage de l'utilisation moyenne de la mémoire

- **Type de valeur** : Nombre entier
- **Contexte d'exécution** : Utilisateur

```
$os = Get-WmiObject win32_OperatingSystem
$used_memory = $os.totalvisiblememorysize - $os.freephysicalmemory
echo $used_memory
```

Affichage de l'utilisation moyenne de la mémoire virtuelle

- **Type de valeur** : Nombre entier
- **Contexte d'exécution** : Utilisateur

```
$os = Get-WmiObject win32_OperatingSystem
$used_memory = $os.totalvirtualmemorysize - $os.freevirtualmemory
echo $used_memory
```

Affichage de l'utilisation moyenne du réseau

- **Type de valeur** : Nombre entier
- **Contexte d'exécution** : Utilisateur

```
$Total_bytes=Get-WmiObject -class Win32_PerfFormattedData_Tcpip_NetworkInterfac
e
|Measure-Object -property BytesTotalPersec -Average |Select-Object -ExpandPrope
rty Average
echo ([System.Math]::Round($Total_bytes))
```

Affichage de l'utilisation moyenne de la mémoire pour un processus

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$PM = get-process chrome |Measure-object -property PM -Average|Select-Object -E
xpandProperty Average
$NPM = get-process chrome |Measure-object -property NPM -Average|Select-Object
-ExpandProperty Average
echo [System.Math]::Round(($PM+$NPM)/1KB)
```

Vérification de l'exécution ou de la non-exécution d'un processus

- **Type de valeur** : Booléen(ne)
- **Contexte d'exécution** : Utilisateur

```
$chrome = Get-Process chrome -ea SilentlyContinue
      i f ( $ c h r o m e ) {
           e c h o    $ t r u e
                      }
          e l s e {
          e c h o    $ f a l s e
                      }
```

Vérification de l'activation du démarrage sécurisé

- **Type de valeur** : Booléen(ne)
- **Contexte d'exécution** : Administrateur

```
try { $bios=Confirm-SecureBootUEFI }
catch { $false }
echo $bios
```

Interface réseau active

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$properties = @('Name','InterfaceDescription')
$physical_adapter = get-netadapter -physical | where status -eq "up"
|select-object -Property $properties
echo $physical_adapter
```

Vérification de la version de PowerShell

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$x = $PSVersionTable.PSVersion
echo "$($x.Major).$($x.Minor).$($x.Build).$($x.Revision)"
```

Vérification de la capacité maximale de la batterie

- **Type de valeur** : Nombre entier
- **Contexte d'exécution** : Utilisateur

```
$max_capacity = (Get-WmiObject -Class "BatteryFullChargedCapacity" -Namespace "
ROOT\WMI").FullChargedCapacity | Measure-Object -Sum |
Select-Object -ExpandProperty Sum
echo $max_capacity
```

Vérification de l'état de charge de la batterie

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$charge_status = (Get-CimInstance win32_battery).batterystatus
$charging = @(2,6,7,8,9)
if($charging -contains $charge_status[0] -or $charging -contains $charge_status
[1] )
{
                echo "Charging"
                }else{
                echo "Not Charging"
}
```

Profil de gestion de l'alimentation actif

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Administrateur

```
$plan = Get-WmiObject -Class win32_powerplan -Namespace root\cimv2\power
-Filter "isActive='true'"
echo $plan
```

Vérification de la présence d'un réseau sans fil

- **Type de valeur** : Booléen(ne)
- **Contexte d'exécution** : Utilisateur

```
$wireless = Get-WmiObject -class Win32_NetworkAdapter -filter "netconnectionid
like 'Wi-Fi%'"
 if($wireless){echo $true}
```

```
else {echo $false}
```

Obtention de la version Java

- **Type de valeur** : Chaîne
- **Contexte d'exécution** : Utilisateur

```
$java_ver = cmd.exe /c "java -version" '2>&1'
echo $java_ver
```

Créer un capteur pour les terminaux Windows Desktop

Créez des Capteurs dans Workspace ONE UEM Console pour effectuer le suivi d'attributs spécifiques des terminaux, tels que la batterie restante, la version du système d'exploitation ou l'utilisation moyenne du CPU. Chaque capteur inclut un script de code pour collecter les données souhaitées. Vous pouvez télécharger ces scripts ou les entrer directement dans la console.

Les Capteurs utilisent des scripts PowerShell pour collecter des valeurs d'attributs. Vous devez créer ces scripts vous-même avant de créer un capteur ou pendant la configuration dans la fenêtre de script.

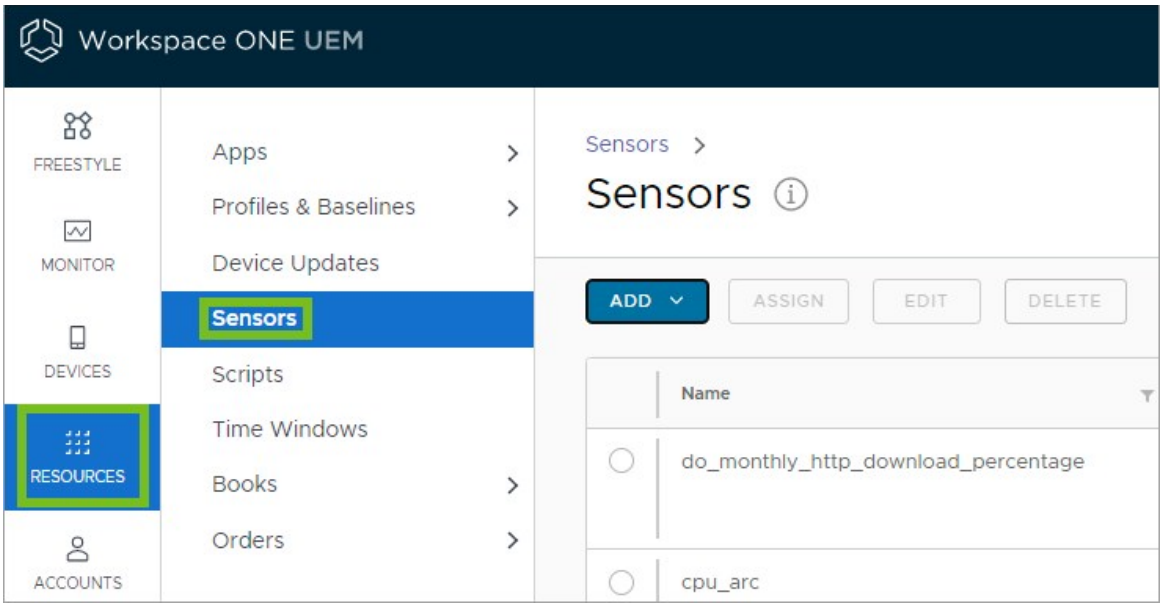
Chaque script contient un seul capteur. Si un script renvoie plusieurs valeurs, Workspace ONE Intelligence et Workspace ONE UEM lisent uniquement la première valeur de la réponse du script. Si un script renvoie une valeur null, Workspace ONE Intelligence et Workspace ONE UEM ne signalent pas le capteur.

Conditions prérequises

Si vous souhaitez afficher des Capteurs pour plusieurs terminaux et interagir avec les données dans des rapports et des tableaux de bord, vous devez activer Workspace ONE Intelligence. Si vous souhaitez afficher les données des Capteurs d'un seul terminal, vous n'avez pas besoin de Workspace ONE Intelligence. Accédez à la page **Détails du terminal** et sélectionnez l'onglet **Capteurs** pour afficher les données.

Procédure

1. Accédez à **Ressources** > **Capteurs** > **Ajouter**.



2. Sélectionnez **Windows**.
3. Configurez les paramètres du capteur dans l'onglet **Général**.
   - **Nom** : entrez le nom du capteur. Le nom doit commencer par une lettre minuscule suivie de caractères alphanumériques et de traits de soulignement. Le nom doit comporter entre 2 et 64 caractères. N'utilisez pas d'espaces dans cet élément de menu.
   - **Description** : entrez la description du capteur.
4. Sélectionnez **Suivant**.
5. Configurez les paramètres du capteur dans l'onglet **Détails**.
   - **Langage** : Workspace ONE UEM prend en charge PowerShell.
   - **Contexte d'exécution** : ce paramètre contrôle si le script du capteur s'exécute dans un contexte utilisateur ou système.
   - **Architecture d'exécution** : ce paramètre contrôle si le script du capteur s'exécute sur un terminal basé sur l'architecture. Vous pouvez limiter l'exécution du script sur les terminaux 32 bits ou 64 bits uniquement ou exécuter le script en fonction de l'architecture du terminal. Vous pouvez également forcer le script à s'exécuter en 32 bits, quel que soit le terminal.
   - **Type de données de réponse** : sélectionnez le type de réponse au script du capteur. Vous pouvez choisir entre :
     - **Chaîne**
     - **Nombre entier**
     - **Booléen(ne)**
     - **Date Heure**
   - **Commande de script** : téléchargez un script pour le capteur ou écrivez-en un dans la zone de texte fournie.
6. Sélectionnez **Enregistrer** pour attribuer vos Capteurs ultérieurement ou sélectionnez **Enregistrer et attribuer** pour attribuer les Capteurs à des terminaux dans des groupes.

7. Pour poursuivre l'attribution, sélectionnez **Ajouter une attribution**.
8. Dans l'onglet **Définition**, entrez le **Nom de l'attribution** et utilisez l'élément de menu **Sélectionner un Smart Group** pour sélectionner le groupe de terminaux dont vous souhaitez collecter les données des Capteurs.
9. Dans l'onglet **Déploiement**, sélectionnez le déclencheur pour que le capteur signale l'attribut du terminal. Vous pouvez sélectionner plusieurs valeurs.

Étapes suivantes

Après la création d'un capteur, utilisez la page **Détails du terminal** dans Workspace ONE UEM pour afficher les données de terminaux individuels ou accédez à Workspace ONE Intelligence pour utiliser des rapports et des tableaux de bord afin d'interagir avec les données de plusieurs terminaux.

Automatiser les configurations de point de terminaison à l'aide de scripts pour les terminaux Windows Desktop

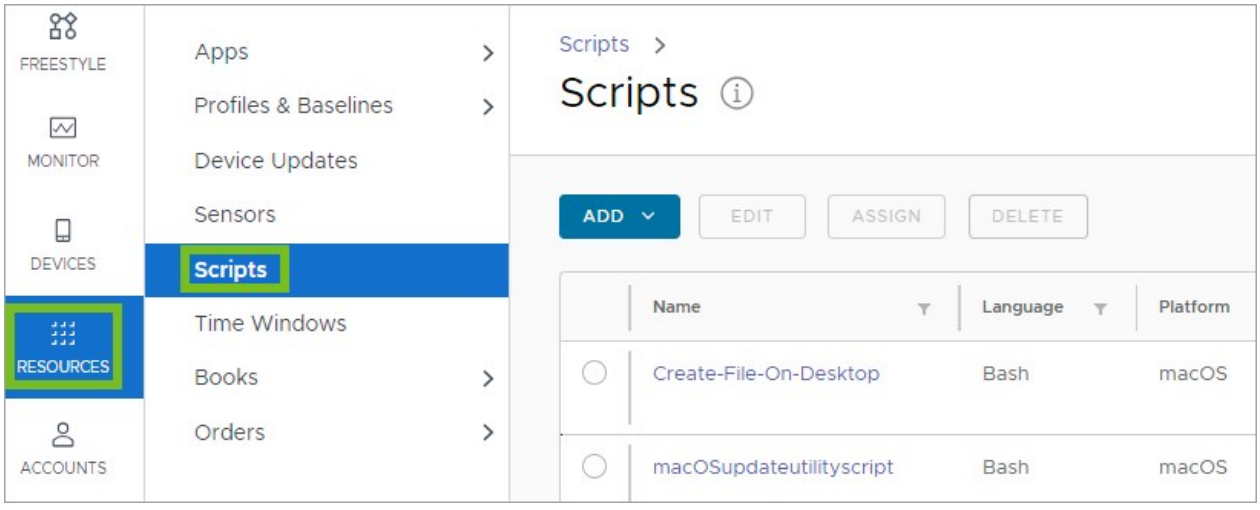
Utilisez des Scripts pour exécuter le code PowerShell pour les configurations de point de terminaison sur les terminaux Windows Desktop à l'aide de Workspace ONE UEM.

Fonctionnalité Freestyle

Scripts est une fonctionnalité Freestyle disponible pour les environnements SaaS. Pour plus d'informations sur Freestyle, accédez à Freestyle Orchestrator.

Description des Scripts

Les Scripts, situés dans la navigation principale sous **Ressources**, permettent de transférer du code vers des terminaux Windows pour exécuter divers processus. Par exemple, vous pouvez déployer un script PowerShell qui invite les utilisateurs à redémarrer leur terminal.

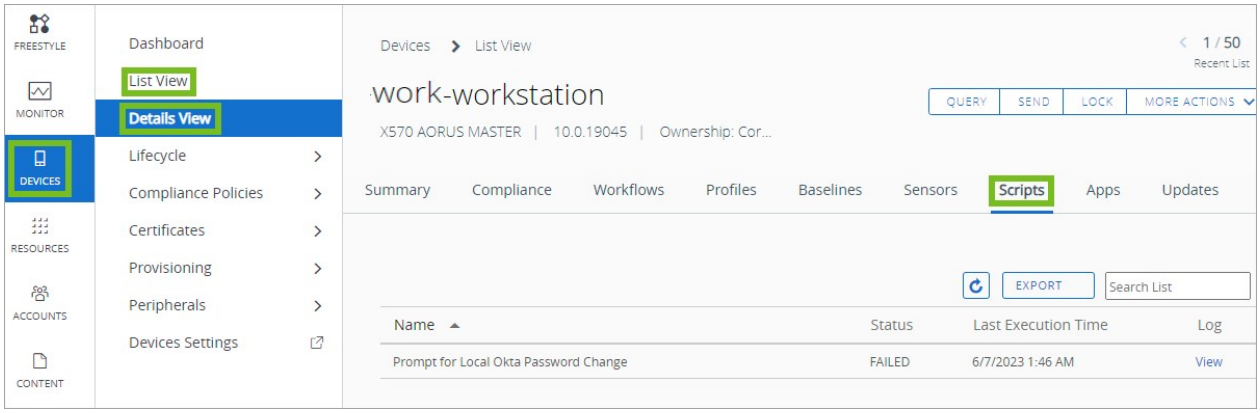


Utilisez des **variables** dans vos scripts pour protéger les données statiques sensibles, telles que les mots de passe et les clés d'API, ou utilisez des valeurs de recherche pour les données dynamiques telles que l'ID de terminal et le nom d'utilisateur. Vous pouvez également autoriser vos utilisateurs Windows à accéder à ce code pour qu'ils puissent l'exécuter sur leurs terminaux lorsque cela est nécessaire. Pour rendre le code disponible, intégrez Workspace ONE Intelligent Hub aux Scripts de sorte que les utilisateurs puissent accéder au code dans la zone Applications du catalogue.

Important : Les Scripts ne sont pas autorisés à être attribués à des terminaux personnels pour des raisons de confidentialité.

Comment savoir si vos Scripts s'exécutent avec succès ?

Vous pouvez déterminer si les Scripts s'exécutent avec succès à partir de l'onglet **Scripts** de la page Détails du terminal. Dans Workspace ONE UEM Console, accédez au groupe organisationnel applicable, sélectionnez **Terminaux** > **Affichage en liste**, puis sélectionnez le terminal applicable. Dans l'onglet **Scripts**, dans la colonne État, recherchez l'état **Exécuté** ou **Échec**. Les états dépendent du code de sortie (également appelé code d'erreur ou code de retour).



- Exécuté : Workspace ONE UEM affiche cet état lorsque le code de sortie renvoie 0.
- Échec : Workspace ONE UEM affiche cet état lorsque le code de sortie renvoie une valeur différente de 0.

Créer un script pour les terminaux Windows Desktop

Les Scripts pour Windows Desktop géré par Workspace ONE UEM prennent en charge l'utilisation de PowerShell pour exécuter des codes sur les terminaux des utilisateurs finaux. Intégrez des Scripts à Workspace ONE Intelligent Hub pour Windows et activez le libre-service pour les Scripts de vos utilisateurs.

Remarque : Si vous publiez des scripts sur moins de 2000 terminaux inférieurs (valeur par défaut), les terminaux sont immédiatement invités à extraire la ressource. Cependant, si les Smart Group attribués disposent de plus de 2000 terminaux, les terminaux recevront la ressource la prochaine fois qu'ils se connecteront à Workspace ONE UEM Console.

Procédure

1. Accédez à **Ressources > Scripts > Ajouter**.
2. Sélectionnez **Windows**.
3. Configurez les paramètres des scripts dans l'onglet **Général**.

Paramètre	Description
Nom	Entrez le nom du script.
Description	Entrez la description du script.

Paramètre	Description
Personnalisation du catalogue d'applications	Activez l'offre d'accès en libre-service aux Scripts dans le catalogue de Workspace ONE Intelligent Hub. **Nom d'affichage** : entrez le nom que les utilisateurs voient dans le catalogue. **Description de l'affichage** : entrez une brève description de l'action du script. **Icône** : téléchargez une icône pour le script. **Catégorie** : sélectionnez une catégorie pour le script. Les catégories aident les utilisateurs à filtrer les applications dans le catalogue. Bien que vous ayez fini de configurer les paramètres du script dans le catalogue, une autre configuration doit être définie pour afficher votre script dans Workspace ONE Intelligent Hub. Lorsque vous attribuez le script à des terminaux, activez l'élément de menu **Afficher dans le Hub** pour que ces personnalisations s'affichent dans le catalogue.

4. Configurez les paramètres du script dans l'onglet Détails.

Paramètre	Description
Langue	Workspace ONE UEM prend en charge PowerShell.
Contexte d'exécution	Ce paramètre contrôle si le script s'exécute dans le contexte utilisateur ou système.
Architecture d'exécution	Ce paramètre contrôle si le script s'exécute sur un terminal basé sur l'architecture. Vous pouvez limiter l'exécution du script sur les terminaux 32 bits ou 64 bits uniquement ou exécuter le script en fonction de l'architecture du terminal. Vous pouvez également forcer le script à s'exécuter en 32 bits, quel que soit le terminal.
Délai d'expiration	Si le script s'exécute en boucle ou qu'il ne répond pas pour une raison quelconque, entrez la durée en secondes pendant laquelle le système doit exécuter le script avant de l'arrêter.
Code	Téléchargez un script ou écrivez-en un dans la zone de texte fournie.

5. Sélectionnez **Suivant** pour configurer l'onglet **Variables**.

   Ajoutez des valeurs statiques, telles que des clés d'API, des noms de compte de service ou un mot de passe, en indiquant la clé et la valeur de la variable. Vous pouvez aussi ajouter des valeurs dynamiques telles que **enrollmentuser** en indiquant une clé, puis en sélectionnant l'icône de valeur de recherche. Pour utiliser des variables dans un script, référencez-les à l'aide de `$env:key`. Par exemple, si la définition de la variable comprend une clé nommée **SystemAccount** et la valeur admin01, le script peut attribuer la variable à un compte de variable de script nommé via la référence `$account = $env:SystemAccount`.

6. Pour attribuer des Scripts à des terminaux, sélectionnez le script, choisissez **Attribuer**, puis sélectionnez **Nouvelle attribution**.

7. Dans l'onglet **Définition**, entrez le **Nom de l'attribution** et utilisez l'élément de menu **Sélectionner un Smart Group** pour sélectionner le groupe de terminaux auxquels vous souhaitez envoyer les Scripts.

8. Dans l'onglet **Déploiement**, pour **Déclencheurs**, sélectionnez le déclencheur qui démarre le script. Vous pouvez sélectionner plusieurs déclencheurs.

9. Activez **Afficher dans le Hub** pour afficher les paramètres de **Personnalisation du catalogue**

d'applications pour le script dans Workspace ONE Intelligent Hub. Vous pouvez désactiver cette option pour masquer un script aux utilisateurs du catalogue.

Étapes suivantes

Accédez à l'onglet **Scripts** dans les **Détails du terminal** d'un terminal pour afficher l'état de vos Scripts.

Dell Command | Product Integrations

Intégrez Workspace ONE UEM avec les produits Dell Command | (Dell Command | Configure, Dell Command | Monitor et Dell Command | Update) pour configurer les paramètres BIOS du terminal, paramétrer les informations collectées par Workspace ONE UEM sur les terminaux Dell Enterprise et activer la mise à jour des microprogrammes, des pilotes et des applications.

Dell Command | Configure

L'intégration de Workspace ONE UEM à Dell Command | Configure vous permet d'améliorer la gestion des terminaux et d'activer toutes les fonctionnalités du profil BIOS pour les terminaux Windows Desktop sur vos terminaux Dell Enterprise. Le profil BIOS peut contrôler la virtualisation matérielle et la sécurité du BIOS.

Dell Command | Monitor

Intégrez Workspace ONE UEM à Dell Command | Monitor afin d'améliorer les informations collectées par Workspace ONE UEM à partir de terminaux Dell Enterprise enrôlés. Pour utiliser le profil BIOS, vous devez ajouter cette intégration à votre environnement. Cette intégration vous permet de configurer les paramètres du BIOS du terminal afin de contrôler la virtualisation matérielle et la sécurité du BIOS. Vous devez également activer la distribution logicielle afin de déployer Dell Command | Monitor sur vos terminaux. Configurez le profil BIOS pour activer Dell Command | Monitor.

État d'intégrité de la batterie

L'intégrité générale d'une batterie a un impact sur la durée de vie d'un terminal. Grâce à Dell Command | Monitor et WinAPI, surveillez l'intégrité des batteries de vos terminaux professionnels Dell. Cette intégrité ne montre pas le niveau de charge en cours de la batterie mais remonte l'habilité à tenir une charge, le temps nécessaire à obtenir une charge complète et d'autres facteurs sous forme de pourcentages. Selon Dell, toute batterie avec un état inférieur à 25 % devrait être remplacée.

Dell Command | Update

L'intégration de Workspace ONE UEM à Dell Command | Update vous permet de contrôler quels types de mises à jour déployer sur vos terminaux et à quel moment. Ce logiciel de gestion côté client permet la mise à jour du microprogramme, des pilotes et des applications pour les terminaux Dell pris en charge. Configurez le profil Mises à jour OEM pour activer Dell Command | Update sur les terminaux des utilisateurs finaux.

Configurer Dell Command | Products dans Workspace ONE UEM

Pour améliorer la gestion de vos terminaux Dell Enterprise, ajoutez Dell Command | Products dans Workspace ONE UEM Console.

Pour en savoir plus sur la création d'un fichier MSI, consultez la rubrique de la documentation Dell Comment créer un module de mise à jour MSI Dell Command Update.

Vous pouvez choisir d'utiliser le programme d'installation pour automatiser ce processus ou vous pouvez installer à partir de la ligne de commande. Lors de l'utilisation du programme d'installation, cliquez sur le bouton **Extraire**, puis cliquez sur **Installer**. Pour installer à partir de la ligne de commande :

Conditions prérequises

Vous devez activer la distribution logicielle afin de déployer Dell Command | Products sur vos terminaux. Pour plus d'informations sur les fichiers du module et la distribution de logiciels, consultez la rubrique Charger et configurer les fichiers Win32 pour la distribution de logiciels.

Téléchargez la dernière version de Dell Command | Products pour continuer : - Dell Command | Configure - Dell Command | Update - Dell Command | Monitor

Procédure

1. Ouvrez le fichier .EXE, puis cliquez sur **Extraire**. Enregistrez les fichiers extraits dans un dossier.
2. Naviguez vers le dossier et recherchez le fichier **.MSI**.
3. Dans UEM Console, ajoutez le fichier MSI extrait en tant qu'application interne. Assurez-vous de définir l'Architecture de processeur prise en charge sur 32 ou 64 bits en fonction de l'OS du terminal.
4. Dans l'onglet **Options de déploiement**, définissez les **Privilèges administrateur** sur **Oui**.
5. Ajoutez une attribution de l'application à vos terminaux Dell Enterprise.

Résultats

L'application est importée et installée sur les terminaux attribués, et vous pouvez à présent déployer les profils Mises à jour OEM sur le terminal.

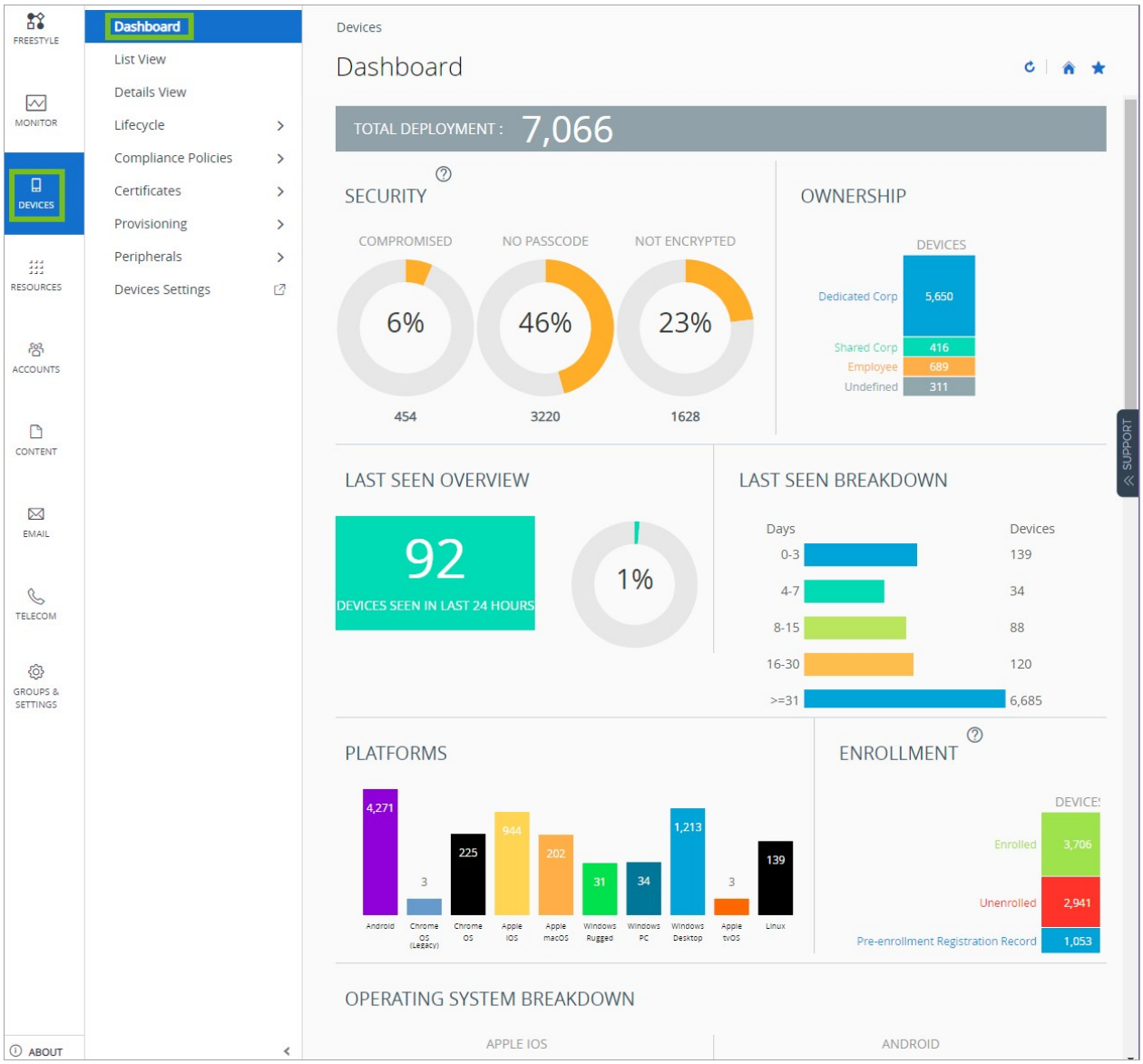
Gestion de terminaux Windows Desktop

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

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

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

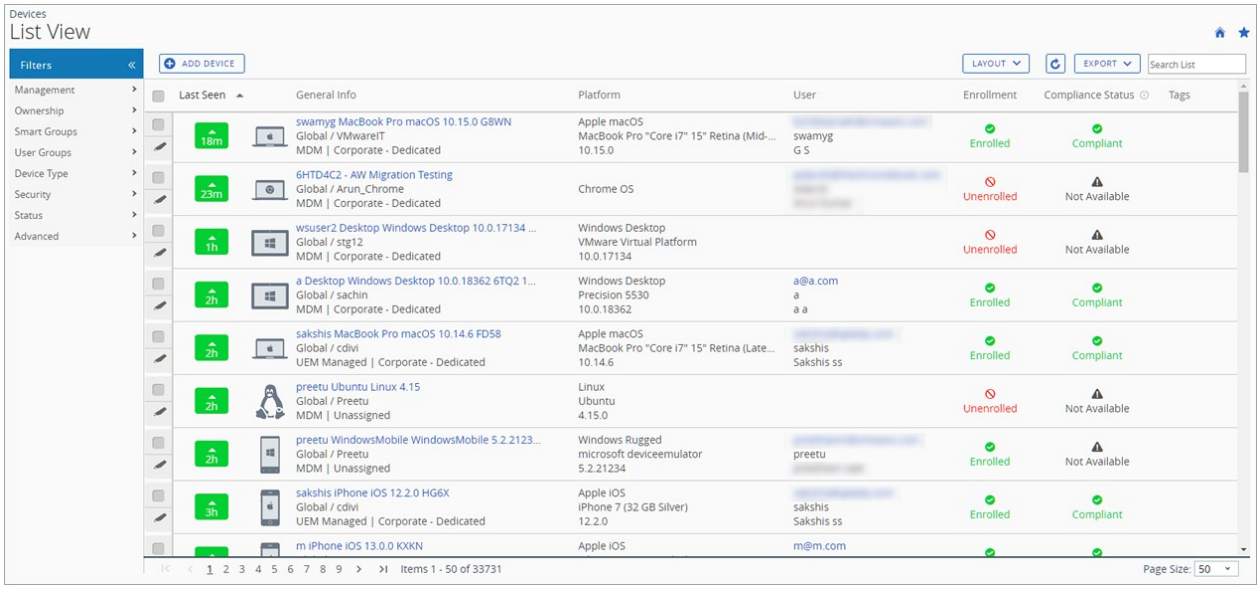
configuré pour la sécurité.

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

Affichage en liste des terminaux

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



La colonne **Dernière connexion** affiche un indicateur signalant le nombre de minutes écoulées depuis que le terminal s'est connecté pour la dernière fois. L'indicateur est rouge ou vert, selon la

durée pendant laquelle le terminal est inactif. La valeur par défaut est de 480 minutes (8 heures), mais vous pouvez définir une valeur personnalisée en accédant à **Groupes et paramètres** > **Tous les paramètres** > **Terminaux et utilisateurs** > **Général** > **Avancé** et en modifiant la valeur de **Délai d'expiration d'inactivité du terminal (en min)**.

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

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

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

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

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

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

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

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

Exporter l'affichage en liste

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

Recherche dans l'affichage en liste des terminaux

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

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

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

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

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

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.

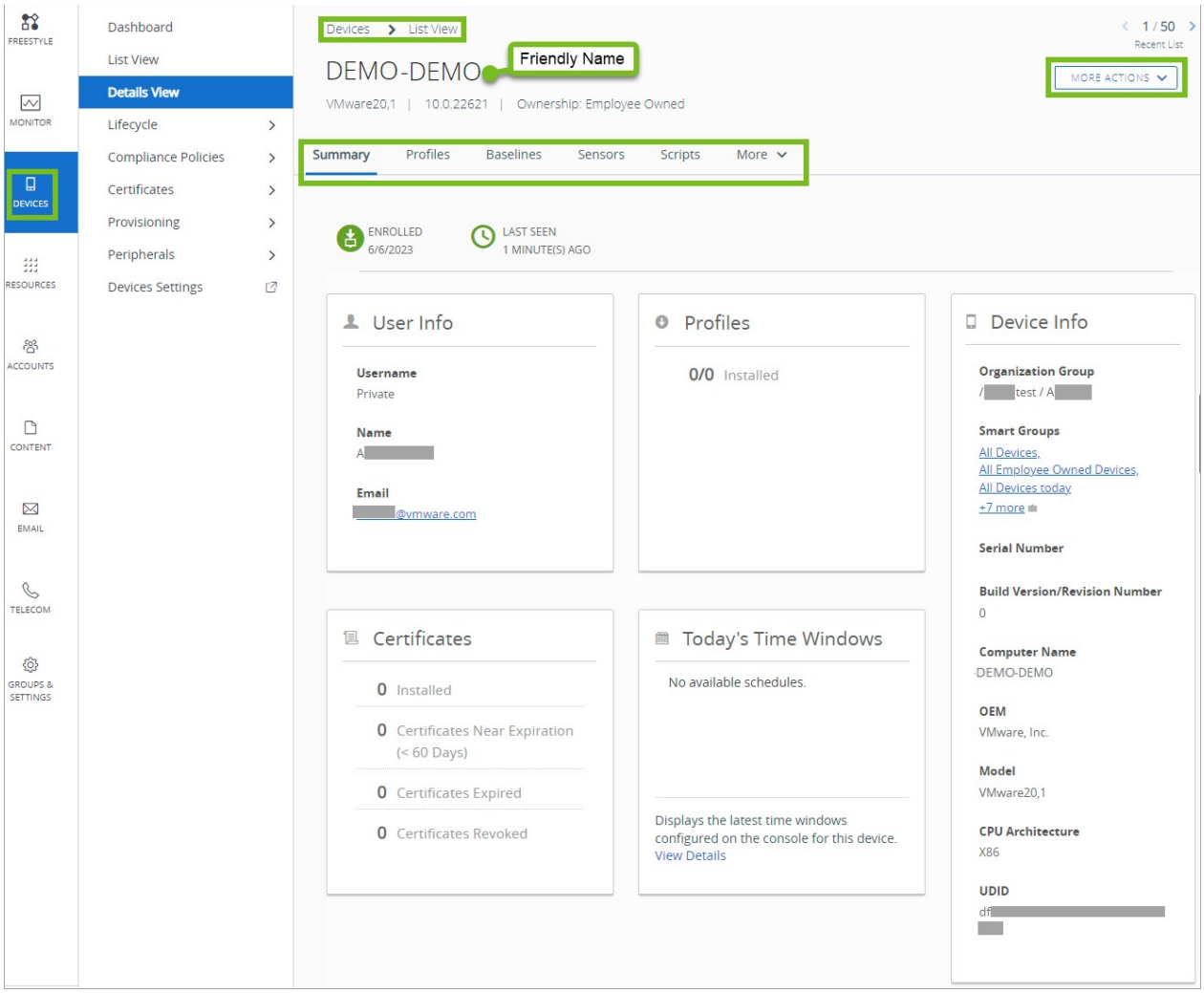
Pour utiliser cette fonctionnalité, vous devez respecter les exigences suivantes :

- 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 Desktop
    - 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.

Détails de la page Terminal Windows Desktop

Utilisez la page Détails du terminal dans Workspace ONE UEM pour suivre les informations détaillées du terminal pour les terminaux Windows Desktop et accéder rapidement aux actions de gestion des utilisateurs et des terminaux. Vous pouvez accéder à la page Détails du terminal en sélectionnant le nom convivial dans la vue Liste des terminaux, à l'aide de l'un des tableaux de bord ou avec l'un des outils de recherche.



Détails du service de notification Windows

Vous pouvez voir l'état des communications du terminal avec le service de notification Windows (WNS) dans l'onglet Réseau de la page Détails du terminal. Le service de notification Windows (WNS) prend en charge l'envoi de notifications à vos terminaux. Il n'est pas utilisé pour les informations sensibles. Si un terminal n'est pas en ligne, le service met en cache les notifications jusqu'à ce que le terminal se connecte à nouveau. Pour plus d'informations sur le service de notification Windows (WNS), consultez la rubrique Prise en charge des notifications Push pour la gestion des terminaux.

Les états de WNS incluent les éléments suivants :

- **État du serveur WNS** – Affiche l'état de votre serveur WNS.
- **Dernière demande de renouvellement WNS** – Date et heure de la dernière tentative de renouvellement de la connexion du service de notification Windows au terminal. Cette connexion permet à Workspace ONE UEM d'interroger le terminal et d'y transférer des stratégies (sous réserve des conditions de mise en réseau, de détection de la batterie et de détection des données).
- **Demande GET WNS suivante** : Date et heure de la prochaine tentative planifiée de renouvellement de la connexion de WNS au terminal.
- **URI de canal WNS** : Point de terminaison de communication WNS utilisé par les terminaux

et Workspace ONE UEM. Ce point de terminaison utilise le format suivant : `https://*.notify.windows.com/?token=_{TOKEN}`.

Plus d'actions

Le menu déroulant **Plus d'actions** de la page **Détails du terminal** vous permet d'effectuer des actions à distance sur le terminal sélectionné.

Les actions varient selon différents facteurs, tels que les paramètres de Workspace ONE UEM Console ou le statut d'enrôlement :

- **Applications (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir la liste des applications installées.

  L'action Applications (Requête) nécessite une connexion active d'utilisateur enrôlé.

- **Lignes de base (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir la liste des échantillons.

- **Certificats (Requête)** – Envoyez une requête MDM au terminal pour recevoir une liste des certificats installés.

  L'action Certificats (Requête) nécessite une connexion active d'utilisateur enrôlé.

- **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 l'action en masse. Utilisez 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 code secret** : modifiez le mot de passe d'un terminal Windows Desktop enrôlé avec un utilisateur de base. Cet élément de menu ne prend pas en charge les services d'annuaire. Lorsque vous choisissez d'utiliser cette option, Workspace ONE UEM génère un nouveau mot de passe et l'affiche dans Workspace ONE UEM Console. Utilisez le nouveau mot de passe pour déverrouiller le terminal.

- **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.

- **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**.

- **Réinitialisation entreprise** – Rétablissez les paramètres d'usine du terminal en conservant uniquement l'enrôlement Workspace ONE UEM.

  La Réinitialisation 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.
  - Utilisez l'élément de menu **Conserver les applications sur le terminal** dans l'assistant **Effacement des données professionnelles** si vous souhaitez conserver des applications gérées sur vos terminaux Windows. Cette fonctionnalité est utile si vous souhaitez enrôler rapidement un terminal pour un nouvel utilisateur et que vous ne souhaitez pas attendre l'installation d'applications volumineuses sur le terminal Windows réattribué. Vous ne pouvez pas accéder à cette fonctionnalité, sauf si vos terminaux et applications Windows répondent à ces exigences.
    - L'agent de déploiement d'application doit être installé sur la machine Windows.
      - Workspace ONE UEM active la fonctionnalité **Distribution logicielle** par défaut pour les déploiements SaaS et sur site. La fonctionnalité **Distribution logicielle** déploie automatiquement l'agent de déploiement d'application vers les terminaux Windows gérés dans votre environnement Workspace ONE UEM. Si vous avez désactivé cette fonctionnalité, vous devez la réactiver pour vous assurer que la dernière version de l'agent de déploiement d'application est déployée sur les terminaux.
      - La console envoie la dernière version de l'agent de déploiement d'application avec chaque mise à jour de la console et les terminaux reçoivent la mise à jour automatiquement.
      - La colonne **Conserver les applications sur le terminal** de l'assistant Effacement des données professionnelles indique si vos terminaux respectent les conditions requises pour utiliser la fonctionnalité.
    - Les applications que vous souhaitez conserver sur les terminaux après un effacement des données professionnelles doivent être gérées dans Workspace ONE UEM. Cette fonctionnalité ne fonctionne pas pour les applications non gérées.

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

- **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.
- **Verrouiller le terminal** – Envoyez une commande MDM pour verrouiller un terminal sélectionné, le rendant inutilisable jusqu'à ce qu'il soit déverrouillé.

  Important : lors du verrouillage d'un terminal, un utilisateur enrôlé doit être connecté au terminal pour que la commande soit traitée. La commande de verrouillage verrouille le terminal et tout utilisateur connecté doit se réauthentifier à l'aide de Windows. Tant qu'un utilisateur enrôlé est connecté au terminal, une commande de verrouillage verrouille le terminal. Si un utilisateur enrôlé n'est pas connecté, la commande de verrouillage du terminal n'est pas traitée.
- **Tout interroger** – Envoyez une requête au terminal pour recevoir une liste du contenu installé : applications (dont Workspace ONE Intelligent Hub, le cas échéant), livres, certificats, informations sur le terminal, profils et mesures de sécurité.
- **Redémarrer le terminal** – Redémarrez un terminal 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.
- **Réparer le Hub** – Réparez VMware Workspace ONE Intelligent Hub sur les terminaux Windows pour rétablir la communication entre la console et le terminal.

  Certains événements peuvent affecter la communication entre le terminal et la console. Certains exemples entrainent l'arrêt des services clés Workspace ONE UEM, la suppression ou la corruption des fichiers associés à Workspace ONE Intelligent Hub et l'échec des mises à niveau des composants Workspace ONE Intelligent Hub en raison d'interruptions du réseau.

  La commande Réparer le Hub prend des mesures pour remédier à ces problèmes. Une fois le Hub réparé, elle vérifie les commandes pour récupérer HMAC. En cas d'erreurs, elle récupère automatiquement HMAC. La commande Réparer le Hub vérifie également si une mise à niveau de la version existe. Si une mise à jour est détectée et est automatique, les mises à jour du Hub sont activées et le Hub est mis à niveau.
- **Demander la journalisation du terminal** – Demandez le journal de débogage pour le 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 livré 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.
- **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**.
- **Afficher le mot de passe du BIOS** – Affichez le mot de passe du BIOS du terminal que Workspace ONE UEM Console a généré automatiquement. Vous pouvez afficher le **Dernier mot de passe appliqué** et le **Dernier mot de passe envoyé**.
- **Interrompre BitLocker** - Vous pouvez désormais interrompre et reprendre le chiffrement de BitLocker depuis la console. Cette fonctionnalité est particulièrement utile pour les utilisateurs qui ont besoin d'aide pour leur terminal mais qui ne disposent pas des autorisations nécessaires pour gérer BitLocker.

  Quand vous choisissez d'**Interrompre BitLocker** pour un terminal, la console affiche plusieurs options, dont notamment **Nombre de redémarrages**. Définissez le nombre de redémarrages estimés du terminal pour le scénario concerné. Par exemple, pour aider un utilisateur à mettre à jour son BIOS, le système peut avoir besoin de redémarrer deux fois, auquel cas sélectionnez **3**. Cette valeur permet au système de redémarrer une fois de plus avec un chiffrement interrompu, de sorte que le BIOS se met à jour correctement avant la reprise BitLocker.

  Si toutefois vous ignorez combien de redémarrages seront nécessaires à une tâche, sélectionnez une valeur plus élevée. Une fois la tâche terminée, vous pouvez utiliser l'option **Plus d'actions > Reprendre BitLocker**.

Gérer vos terminaux Microsoft HoloLens

Workspace ONE UEM prend en charge l'enrôlement et la gestion des terminaux Microsoft HoloLens. Vous devez utiliser la fonctionnalité d'enrôlement et de gestion native pour gérer vos terminaux Windows HoloLens.

Avant de pouvoir gérer vos terminaux HoloLens à l'aide de Workspace ONE UEM, vous devez appliquer le fichier XML de licence aux terminaux. Si vous utilisez des terminaux HoloLens 1, vous devez appliquer le fichier avant de procéder à l'enrôlement. Pour plus d'informations sur l'application des licences, consultez la rubrique Déverrouiller Windows Holographic for Business. Cette étape n'est pas requise pour les terminaux HoloLens 2.

Enrôlement de vos terminaux HoloLens

Vous pouvez enrôler vos terminaux Microsoft HoloLens dans Workspace ONE UEM à l'aide de la fonctionnalité de gestion native. Vous devez utiliser des méthodes d'enrôlement Windows natives, car les terminaux HoloLens ne prennent pas en charge la fonctionnalité VMware Workspace ONE Intelligent Hub. Procédez à l'enrôlement à l'aide de l'une des procédures d'enrôlement MDM natives, avec ou sans la détection automatique pour Windows.

Gérer vos terminaux HoloLens

Après l'enrôlement, vous pouvez appliquer des profils pris en charge à vos terminaux HoloLens à l'aide de Workspace ONE UEM. Pour voir la liste des fournisseurs de services de configuration (CSP) pris en charge, consultez la rubrique CSP pris en charge dans les terminaux HoloLens.

Gérer et enrôler vos terminaux Arm64

Workspace ONE UEM prend en charge l'enrôlement et la gestion des terminaux ARM64 exécutant Windows 11. Workspace ONE Intelligent Hub est pris en charge sur ARM64 et permet d'enrôler vos terminaux ARM64 à l'aide du Hub ou de l'enrôlement MDM natif. Après l'enrôlement de vos terminaux, vous pouvez déployer et gérer des applications, appliquer des capteurs, des scripts et certains profils à l'aide de Workspace ONE UEM. Tous les profils OMADM et les profils de chiffrement basés sur le Hub sont actuellement pris en charge sur les terminaux ARM64.

Remarque : Les requêtes de capteur basées sur WMI ne sont pas prises en charge sur les périphériques ARM64. Les requêtes basées sur CIM doivent être utilisées à la place. Les requêtes de capteur basées sur CIM sont généralement recommandées pour tous les terminaux Windows.

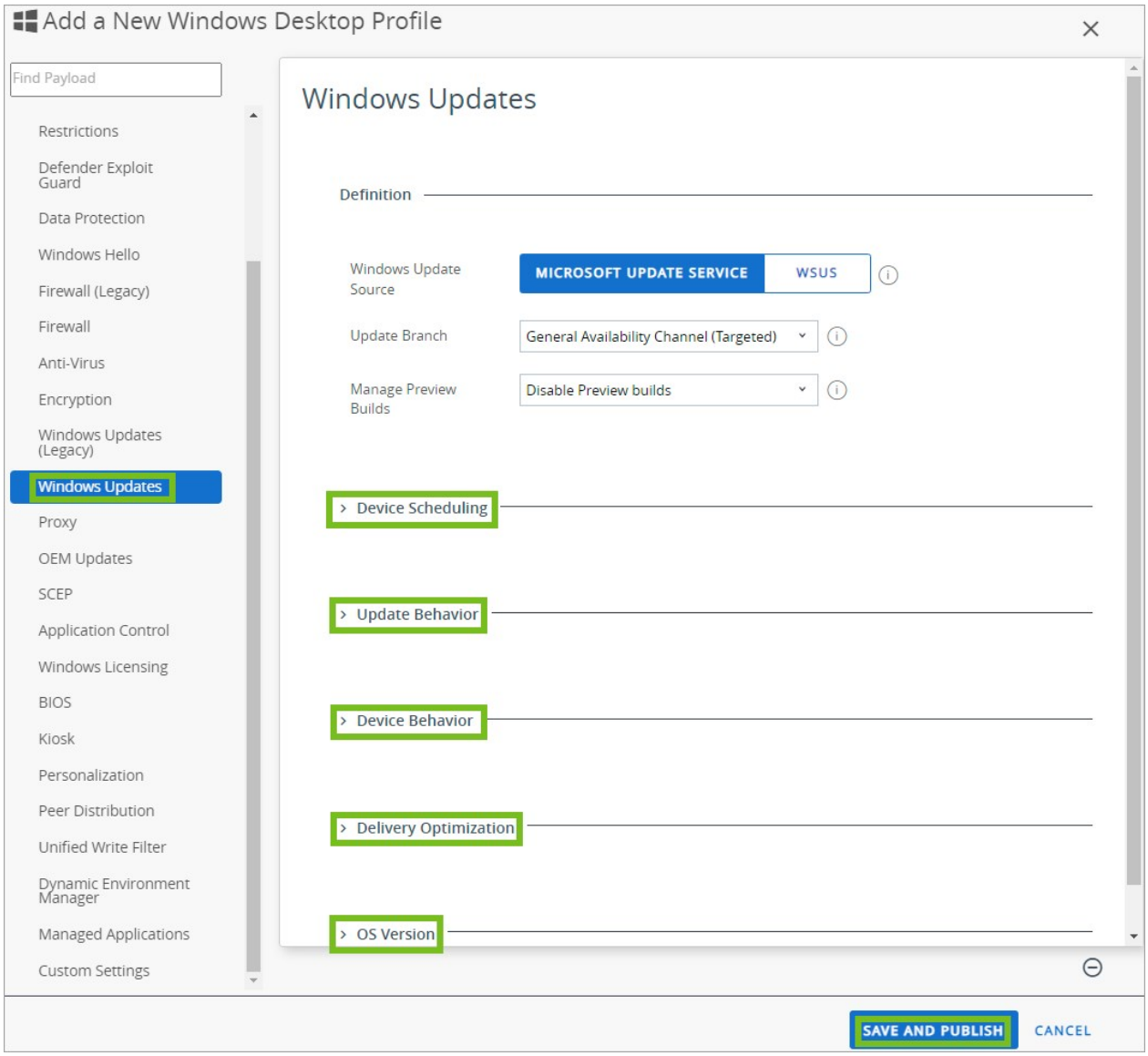
Provisionnement de produit

La configuration de produits vous permet de créer, via Workspace ONE™ UEM, des produits contenant des profils, des applications, des fichiers/actions et des actions d'événement (en fonction de la plateforme utilisée). Ces produits s’appuient sur un ensemble de règles, de planifications et de dépendances pour garantir que vos terminaux sont à jour et disposent du contenu dont ils ont besoin.

La configuration de produits implique également l'utilisation de serveurs relais. Il s'agit de serveurs FTP(S) qui jouent le rôle d'intermédiaires entre les terminaux et Workspace ONE UEM Console. Créez ces serveurs pour chaque stock ou entrepôt afin de stocker le contenu de produits destinés à être distribués sur vos terminaux. Vous trouverez plus d'informations sur la page Provisionnement de produit.

Gestion des mises à jour Windows Device

Les mises à jour du terminal sont maintenant sous le profil du terminal. Dans la console Workspace ONE UEM, accédez à : **Ressources > Profils et lignes de base > Profils > Ajouter > Sélectionner Ajouter un profil > Windows > Windows Desktop > Profil de terminal > Mises à jour Windows**.



Il existe cinq catégories qui peuvent être configurées indépendamment. 1. Planification du terminal 2. Comportement de mise à jour 1. Comportement du terminal 1. Optimisation de la distribution 1. Version du système d'exploitation

Les administrateurs peuvent personnaliser ces paramètres en fonction de leurs besoins spécifiques. Les paramètres les plus fréquemment utilisés sont définis par défaut pour chaque catégorie. En sélectionnant Activer ou Désactiver, vous pouvez configurer ces catégories si nécessaire. N'oubliez pas de sélectionner **Enregistrer et publier** lorsque vous avez terminé la configuration.

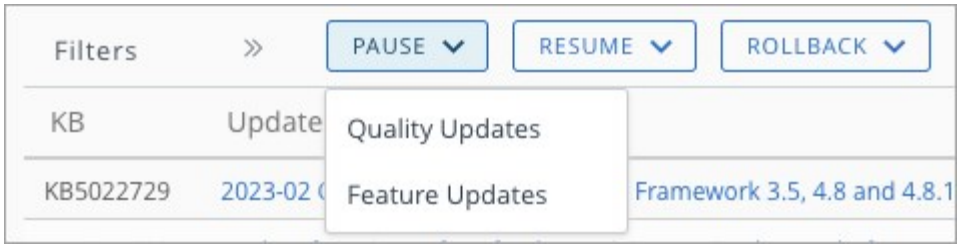
Tableau de bord des mises à jour

Sur l'onglet Mises à jour des détails du terminal, les administrateurs peuvent cliquer sur des mises à jour individuelles pour afficher des métadonnées supplémentaires et voir l'état d'installation de cette mise à jour sur leurs terminaux. Au milieu de la page, des informations sur le déploiement de la stratégie à la fois par la version et par l'état par terminal peuvent être affichées.

Dépannage concernant les mises à jour de fonctionnalités et de qualité

Étant donné que les mises à jour Windows peuvent entraîner des problèmes avec des pilotes ou des

applications spécifiques, trois boutons ont été ajoutés pour aider les administrateurs à dépanner ces situations.



1. Pause : ce bouton permet de suspendre les mises à jour de fonctionnalités et de qualité avant leur sortie (mais seulement pendant 35 jours).
2. Reprendre : ce bouton active à nouveau la recherche et l'installation des mises à jour Windows. Une fois que vous avez repris les mises à jour, vous verrez que le registre pour l'heure de début sera effacé.
3. Restauration : ce bouton permet de revenir temporairement à la version précédent les mises à jour effectuées qui ont causé des problèmes imprévus, le temps que vous résolviez le problème.

Une fois que l'une de ces commandes de bouton est activée, la commande est mise en file d'attente sur le terminal et le journal des événements reste vide. L'état de la commande ne change pas non plus, mais continue à s'afficher comme étant en attente. La Réussite et ou les Échecs s'affichent dans l'onglet Dépannage de la console. Pour toutes les commandes de bouton, 35 jours est la durée maximale autorisée par Microsoft pour tout retard.

Déploiement de configurations de jonction de domaine pour Windows

La jonction de domaine Windows permet à vos utilisateurs de se connecter à un domaine professionnel à distance grâce aux informations d'identification Active Directory ou à celles du terminal local. Utilisez Workspace ONE UEM afin de déployer vos configurations de jonction de domaine de groupe de travail, sur site et hybrides, sur vos terminaux Windows (Windows Desktop).

Intégration à Microsoft Autopilot (jonction de domaine hybride)

Si vous gérez des utilisateurs dans le Cloud et sur site, vous pouvez utiliser Workspace ONE UEM pour attribuer vos configurations de jonction de domaine hybride aux terminaux Windows en exploitant les fonctionnalités de Windows Autopilot et OOBE (Out of Box Experience).

Utiliser un profil Windows Autopilot pour les enrôlements OOBE

Windows Autopilot vous permet de configurer un profil qui spécifie le type de jonction de domaine pour les terminaux passant par OOBE. Vous devez configurer et attribuer un profil Autopilot avec le paramètre de jonction de domaine hybride dans Azure. Les terminaux auxquels ce profil est attribué passeront par le processus OOBE et seront **joints Azure AD hybride**.

Important : si vous n'attribuez pas de profil Autopilot avec la spécification Jonction hybride dans Azure, vos terminaux Windows passeront par OOBE et seront joints Azure AD. Une fois les terminaux joints Azure AD, vous ne pouvez pas initier une jonction de domaine hybride sans réinitialiser complètement les terminaux.

Pour plus de détails sur Autopilot, consultez les rubriques Microsoft | Docs Configurer des profils Autopilot.

- Si vos utilisateurs utilisent un client VPN tiers pour accéder aux ressources (par exemple, les utilisateurs travaillant à domicile), définissez l'élément de menu du profil Autopilot **Ignorer la vérification de connectivité AD (aperçu)** sur **Oui**.
- Si vos utilisateurs n'utilisent pas de client VPN tiers pour accéder aux ressources (par exemple, les utilisateurs se trouvant sur le réseau d'entreprise), définissez l'élément de menu du profil Autopilot **Ignorer la vérification de connectivité AD (aperçu)** sur **Non**.

Configurations requises

- Enrôlement automatique de Windows : Configurez l'enrôlement automatique dans Azure avec Workspace ONE UEM en tant que système de gestion des terminaux mobiles (MDM). Pour plus de détails, consultez la rubrique Configurer Workspace ONE UEM pour utiliser Azure AD comme service d'identité.

- Workspace ONE UEM : Désactivez la page de suivi d'état pour OOBE.
    1. Dans Workspace ONE UEM, rendez-vous dans **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement**.
    2. Sélectionnez l'onglet **Invite facultative**.
    3. Rendez-vous dans la section **Windows** et désactivez **Activer la page de suivi d'état pour OOBE**.
- Abonnement Microsoft : Utilisez l'un des abonnements Microsoft qui prennent en charge l'attribution de licences Windows Autopilot. Consultez l'article dans Microsoft | Docs intitulé Conditions de licence Windows AutoPilot.
- Profil Windows Autopilot : Configurez ce profil dans Azure pour que le paramètre de jonction de domaine hybride soit attribué à vos terminaux Windows. Pour plus de détails, consultez les rubriques Microsoft | Docs Configurer des profils Autopilot.
- Inscrire des terminaux avec le profil Autopilot : Pour plus de détails sur la configuration des terminaux Autopilot, consultez l'article dans Microsoft | Docs intitulé Inscrire manuellement des appareils avec Windows Autopilot.
- AirWatch Cloud Connector (ACC) : Utilisez ACC pour activer la jonction de domaine Active Directory sur site dans Workspace ONE UEM.
- Active Directory Users and Computers (ADUC) : Vous avez besoin du composant logiciel enfichable de la console de gestion Microsoft appelé ADUC pour configurer la jonction de domaine sur site par l'intermédiaire de Workspace ONE UEM.

Conditions

- Vous avez configuré l'enrôlement automatique de Windows avec Azure dans Workspace ONE UEM.
- Vous avez configuré et attribué un profil Autopilot dans Azure afin que les terminaux joignent Azure AD comme étant **joints Azure AD hybride**.
- Vous avez enregistré vos terminaux Windows dans Azure et attribué le profil Autopilot Jonction hybride approprié.
- Vous avez des domaines et des unités d'organisation définis dans Active Directory.
- Vous avez configuré des services d'annuaire dans Workspace ONE UEM Console si vous utilisez Active Directory.
- Vous avez configuré et attribué une configuration de jonction de domaine dans Workspace ONE UEM console.

Ordre des tâches

1. Dans Azure, configurez vos terminaux Autopilot selon les instructions fournies par Microsoft | Docs. Actuellement, ce processus comprend les étapes suivantes.
    1. Enregistrer vos terminaux Autopilot.
    2. Créer un groupe de terminaux.
    3. Créer et attribuer un profil de déploiement Autopilot.

2. Configurez la jonction de domaine sur site dans ADUC, ACC et Workspace ONE UEM.
    1. Dans ADUC, configurez un compte utilisateur disposant d'autorisations de délégué Windows Server, créez une tâche de délégué personnalisée et configurez les autorisations.
    2. Dans ACC, mettez à jour le service AirWatch Cloud Connector pour vous connecter avec le compte utilisateur créé dans ADUC et ajoutez des autorisations d'écriture au dossier ACC.
    3. Dans Workspace ONE UEM, créez une configuration de jonction de domaine pour Active Directory sur site.
    4. Dans Workspace ONE UEM, spécifiez les informations sur l'unité d'organisation en créant et en déployant une ou plusieurs attributions pour la configuration de jonction de domaine.

Première étape : Configurer les terminaux Autopilot

Dans Azure, configurez vos terminaux Autopilot selon la documentation Microsoft. Actuellement, ce processus comprend les étapes suivantes.

1. Créer un groupe de terminaux.
2. Enregistrer vos terminaux Autopilot.
3. Créer et attribuer un profil de déploiement Autopilot.

Deuxième étape : Configurer la jonction de domaine sur site

Les étapes ci-dessous expliquent comment configurer et attribuer une configuration de jonction de domaine dans Workspace ONE UEM. Ces étapes permettent à un terminal de rejoindre un domaine sur site lors de l'enrôlement à Workspace ONE. Lorsqu'ils sont configurés avec un profil Autopilot Jonction hybride, les terminaux passent par OOBE pour joindre Azure AD comme étant **joints Azure AD hybride**. Si vous répondez à toutes les conditions requises pour la jonction de domaine hybride, vous y répondez pour la jonction de domaine sur site, et vous pouvez passer à la configuration, en commençant par la **première étape : Configurer ADUC** dans la section **Jonction de domaine sur site**.

Jonction de domaine sur site

Si vous utilisez Active Directory pour gérer les utilisateurs, vous pouvez utiliser Workspace ONE UEM pour attribuer vos configurations de jonction de domaine sur site.

Configurations requises

- AirWatch Cloud Connector (ACC) : utilisez ACC pour configurer la jonction de domaine pour Active Directory sur site.
- Active Directory Users and Computers (ADUC) : Vous avez besoin du composant logiciel enfichable de la console de gestion Microsoft appelé ADUC pour configurer la jonction de domaine sur site. Ce composant logiciel enfichable fait partie des outils d'administration de serveur distant (RSAT). Consultez Microsoft | Docs pour obtenir la dernière documentation sur Windows Server.

Conditions

- Vous avez des domaines et des unités d'organisation définis dans votre domaine dans Azure.
- Vous avez configuré des services d'annuaire dans Workspace ONE UEM Console si vous utilisez Active Directory. Pour en savoir plus sur la configuration des services d'annuaire, consultez la rubrique Intégration de Workspace ONE UEM à vos services d'annuaire.

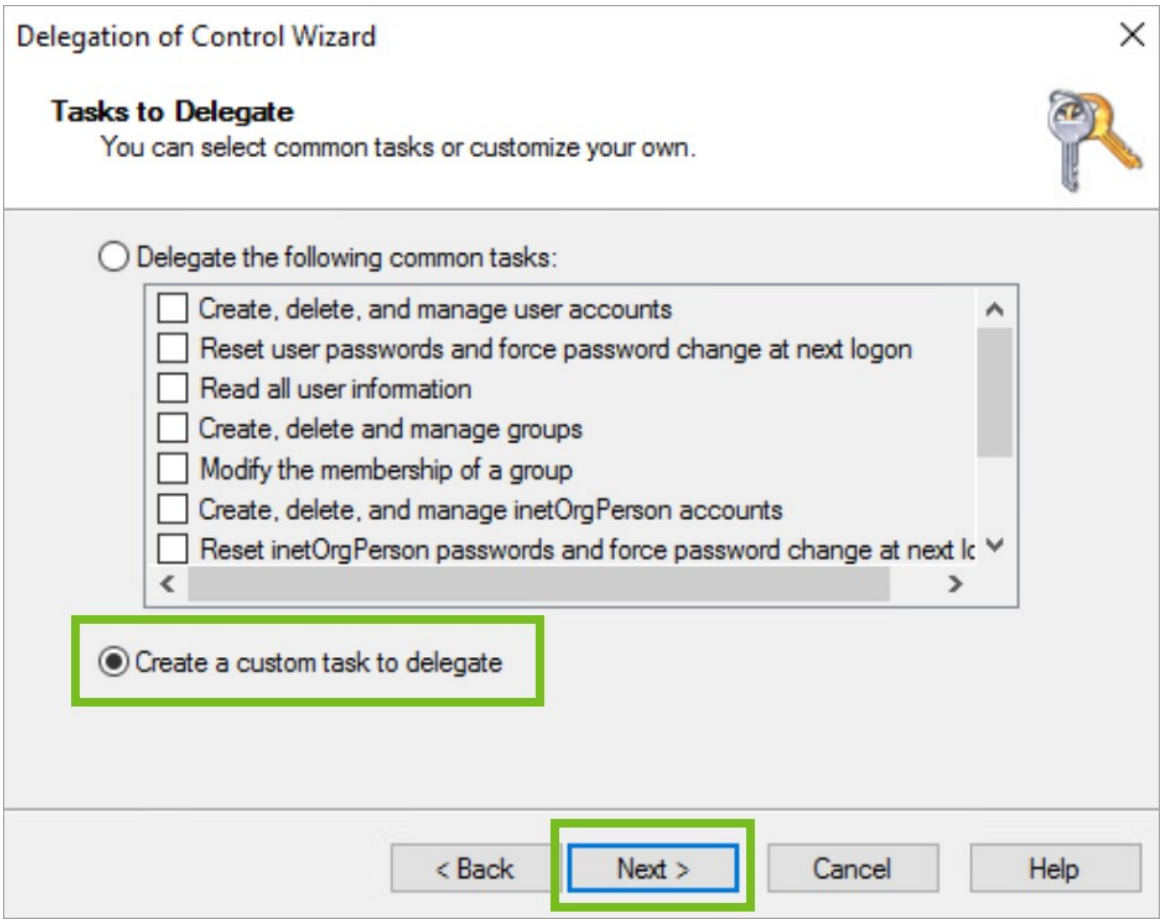
Ordre des tâches

1. Dans ADUC, configurez un compte utilisateur disposant d'autorisations de délégué Windows Server, créez une tâche de délégué personnalisée et configurez les autorisations.
2. Dans ACC, mettez à jour la connexion avec le compte utilisateur créé dans ADUC et ajoutez des autorisations d'écriture. Assurez-vous que l'utilisateur dispose également des privilèges administrateur locaux sur le serveur ACC afin qu'il puisse lancer le service.
3. Dans Workspace ONE UEM, créez une configuration de jonction de domaine pour Active Directory sur site.
4. Dans Workspace ONE UEM, spécifiez les informations sur l'unité d'organisation en créant et en déployant une ou plusieurs attributions pour la configuration de jonction de domaine.

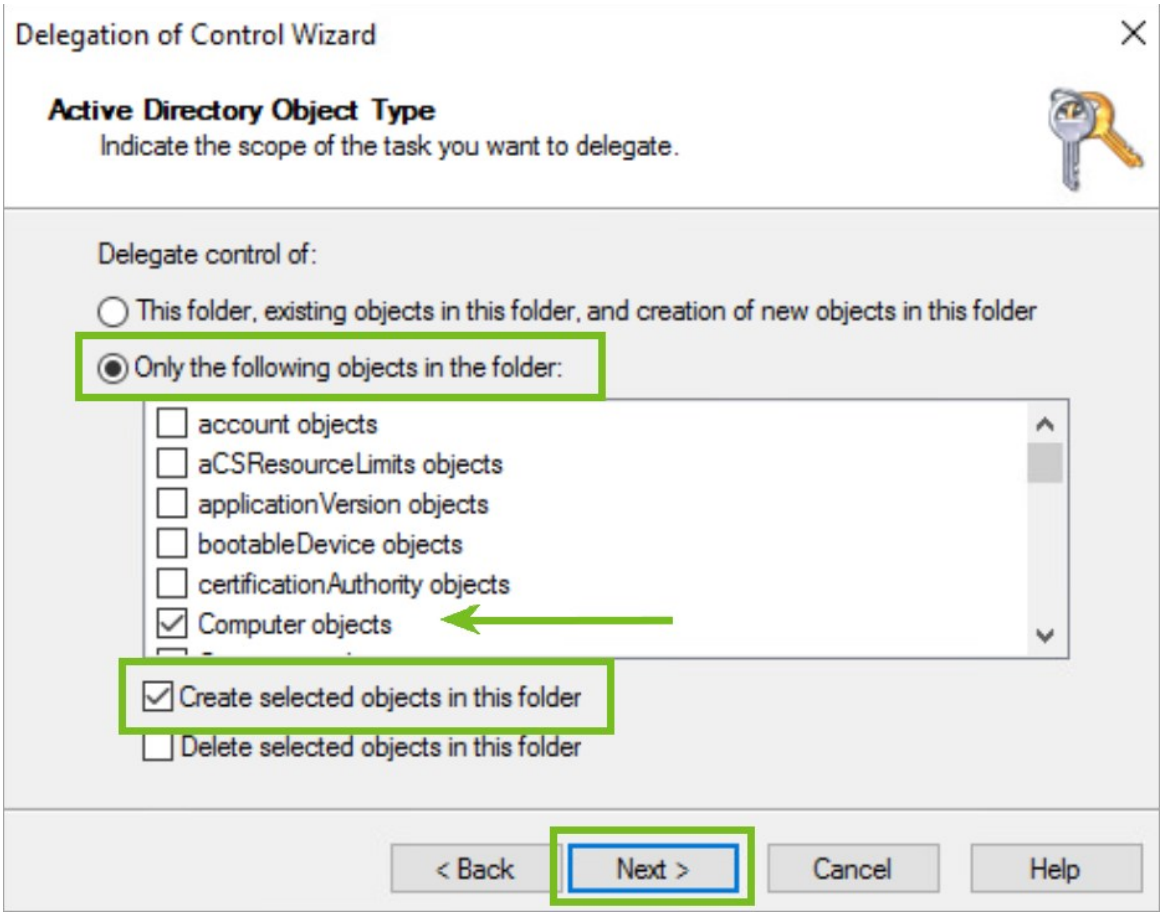
Première étape : Configurer ADUC

Dans ADUC, sélectionnez l'utilisateur disposant d'autorisations de délégué Windows Server, créez une tâche de délégué personnalisée et configurez les autorisations.

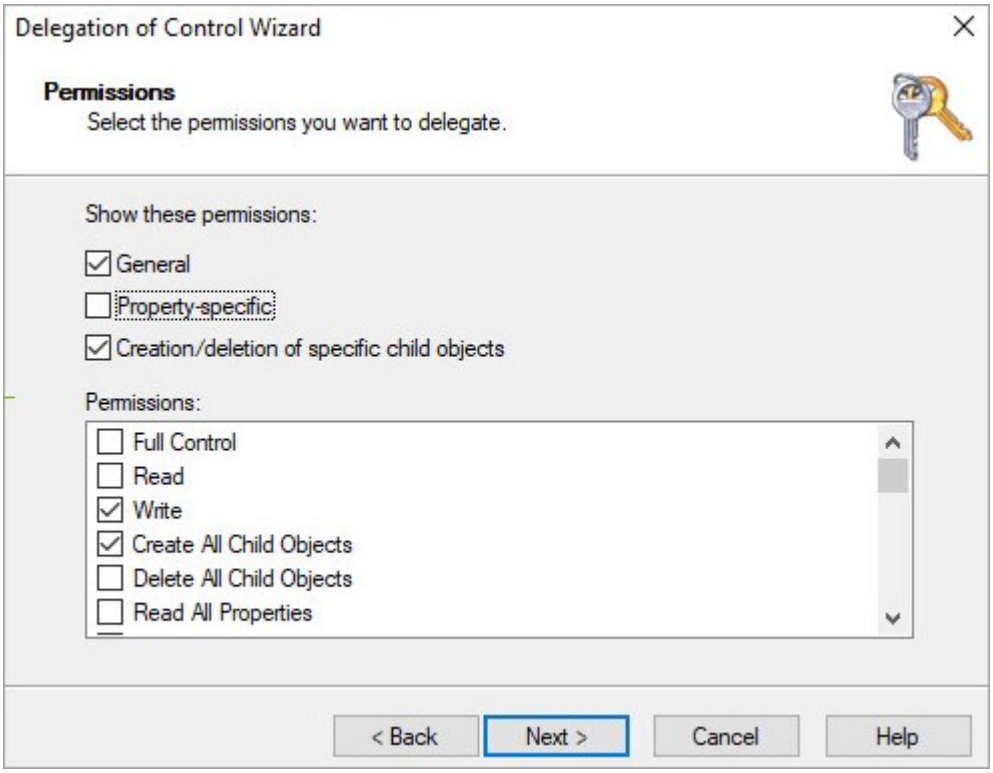
1. Cliquez avec le bouton droit sur le conteneur ou le dossier dans lequel vous souhaitez ajouter les terminaux et sélectionnez **Déléguer le contrôle**. Cette sélection affiche l'**Assistant de délégation de contrôle**.
2. Sélectionnez **Suivant** dans l'**Assistant de délégation de contrôle**.
3. Dans la fenêtre **Utilisateurs ou groupes**, sélectionnez l'utilisateur disposant d'autorisations de délégué Windows Server dans la liste, sélectionnez **Ajouter**, puis sélectionnez **Suivant**. Si ce compte utilisateur n'est pas membre du groupe **Administrateurs de domaine**, augmentez la limite de création de compte d'ordinateur **(ms-ds-machine-account-quota)** de la valeur par défaut de 10 pour éviter les échecs après avoir joint 10 terminaux au domaine.
4. Dans la fenêtre **Tâches à déléguer**, sélectionnez **Créer une tâche personnalisée à déléguer**, puis sélectionnez **Suivant**.



5. Dans la fenêtre **Type d'objet Active Directory**, sélectionnez **Uniquement les objets suivants dans le dossier :**, **Objets ordinateur** et **Créer les objets sélectionnés dans ce dossier**, puis cliquez sur **Suivant**.



6. Dans la fenêtre **Autorisations**, sélectionnez **Général**, **Création/suppression d'objets enfants spécifiques**, **Écriture** et **Créer tous les objets enfants**, puis cliquez sur **Suivant**.



Deuxième étape : Configurer ACC

Mettez à jour la connexion et ajoutez les autorisations d'écriture pour ACC à l'utilisateur modifié dans ADUC afin de déléguer une tâche personnalisée.

1. Modifiez le paramètre **Connexion en tant que** pour ACC à l'utilisateur configuré avec des autorisations de délégué Windows Server.
   Remarque : Assurez-vous que l'utilisateur dispose également des privilèges administrateur locaux sur le serveur ACC afin qu'il puisse lancer le service.
2. Dans la zone **Paramètres de sécurité avancés** d'ACC, accordez à l'utilisateur des autorisations d'**ÉCRITURE** pour le dossier ACC à l'adresse `<Drive>:\VMware\AirWatch\CloudConnector`.

Troisième étape : Créer une jonction de domaine sur site

Déployez une configuration de jonction de domaine dans Workspace ONE UEM sur les terminaux Windows enrôlés qui utilisent les informations d'identification Active Directory pour accéder aux ressources.

1. Dans Workspace ONE UEM Console, accédez à **Groupes et paramètres > Configurations** et sélectionnez **Jonction de domaine** dans la liste.
2. Sélectionnez **Ajouter**.
3. Entrez une valeur dans le champ **Nom** qui vous permette de reconnaître la jonction de domaine. Par exemple, si vos utilisateurs et ordinateurs dans Active Directory suivent un modèle géographique, vous pouvez entrer `Acme - South America`. Cette entrée ne doit pas nécessairement correspondre à des paramètres dans Active Directory, mais l'utilisation de modèles similaires dans les deux systèmes peut aider à organiser vos terminaux dans vos jonctions de domaine.
4. Sélectionnez **Active Directory sur site** pour le **Type de jonction de domaine**.
5. Affichez le **Nom de domaine**. La page de configuration de jonction de domaine entre le nom du **Serveur** configuré sur la page **Services d'annuaire**. La configuration des services d'annuaire Workspace ONE UEM autorise un serveur pour les services d'annuaire, c'est pourquoi ce champ est complété automatiquement. Accédez aux paramètres des services d'annuaire dans **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > Services d'annuaire**.
   Remarque : Si vous souhaitez modifier l'entrée du **Serveur** sur la page **Services d'annuaire**, vous devez **Désactiver** l'élément **DNS SRV** dans le menu.
6. Sélectionnez **Nom convivial du domaine**. La page de configuration de jonction de domaine vous propose une liste de noms conviviaux disponibles ajoutés à la liste de domaines pour votre serveur de services d'annuaire sur la page **Services d'annuaire**. Accédez aux services d'annuaire dans **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > Services d'annuaire**.
7. Entrez votre format préféré pour le nom de la machine dans le champ **Format du nom de la machine**. Utilisez un format pris en charge pour le nom de votre machine. L'infobulle spécifie les formats acceptés. Workspace ONE UEM utilise un maximum de 15 caractères aux formats `%SERIAL%` ou `%RAND:[#]%`.
8. Enregistrez la configuration de jonction de domaine pour l'attribuer ultérieurement ou sélectionnez **Enregistrer et attribuer** maintenant.

Quatrième étape : Attribuer une configuration de jonction de domaine

1. Dans Workspace ONE UEM console, accédez à une page d'attribution en sélectionnant **Attribuer** dans l'affichage en liste de la jonction de domaine dans **Groupes et paramètres > Configurations** et sélectionnez **Jonction de domaine**. Cette fenêtre de configuration s'affiche si vous sélectionnez **Enregistrer et attribuer** pour votre configuration de jonction de domaine.
2. Sélectionnez le nom de la configuration de jonction de domaine, sauf si l'entrée est préremplie.
3. Ajoutez un **Nom de l'attribution** qui vous aidera à identifier l'attribution. L'entrée ne doit pas nécessairement correspondre à un paramètre dans Active Directory.
4. Recherchez les unités d'organisation configurées dans vos paramètres ADUC et sélectionnez-en une.
5. Recherchez et sélectionnez des Smart Groups configurés dans Workspace ONE UEM. Vous pouvez attribuer un Smart Group à une seule unité d'organisation et pas plus. Si vous essayez de sélectionner un Smart Group auquel une unité d'organisation est déjà attribuée, la console affiche un message d'erreur contenant des informations de dépannage, vous permettant de décider quels Smart Groups utiliser pour répondre à votre scénario de déploiement actuel.
6. Créez et enregistrez votre attribution.

Conteneur d'ordinateurs dans les conflits OU/Smart Groups et Active Directory (AD)

Vous pouvez ajouter plusieurs attributions aux configurations de jonction de domaine, mais vous devez prendre en compte la flexibilité des Smart Groups. Étant donné que les Smart Groups sont flexibles, il est possible que vous ayez un terminal dans plusieurs attributions pour une configuration de jonction de domaine. Ce scénario signifie que le terminal est également attribué à plusieurs unités d'organisation, ce qui n'est pas autorisé. Lorsque la console identifie un terminal comme étant dans plusieurs attributions pour une configuration de jonction de domaine, il le place dans le conteneur d'**Ordinateurs** dans Active Directory. Vous pouvez accéder à ADUC et placer le terminal dans l'unité d'organisation souhaitée. Le terminal reçoit la configuration de jonction de domaine qui correspond à l'attribution pour l'unité d'organisation.

Réattribution de jonction de domaine

La configuration de jonction de domaine pour un terminal est évaluée et appliquée pendant le processus d'enrôlement. Une fois qu'un terminal a reçu une configuration de jonction de domaine, vous ne pouvez pas le mettre à jour en modifiant les Smart Groups attribués dans Workspace ONE UEM. Workspace ONE UEM ne fournit qu'une configuration de jonction de domaine au terminal à la fois lors de l'enrôlement.

Joindre un groupe de travail

Si vous avez des utilisateurs qui se servent d'un compte local pour accéder à leurs terminaux et ressources Windows, configurez une jonction vers un groupe de travail Workspace ONE UEM.

Ordre des tâches

1. Dans Workspace ONE UEM, créez une configuration de jonction de domaine pour Joindre un groupe de travail.
2. Dans Workspace ONE UEM, spécifiez le nom du groupe de travail, le format du nom de la machine et les paramètres d'utilisateur local, puis attribuez la configuration à un Smart Group.

Première étape : Créer une jonction de domaine pour les groupes de travail

Déployez une configuration de jonction de domaine dans Workspace ONE UEM pour les terminaux Windows Desktop enrôlés qui utilisent des comptes locaux pour accéder aux ressources.

1. Dans Workspace ONE UEM Console, accédez à **Groupes et paramètres > Configurations** et sélectionnez **Jonction de domaine** dans la liste.
2. Sélectionnez **Ajouter**.
3. Entrez une valeur dans le champ **Nom** qui vous permette de reconnaître la jonction de domaine. Par exemple, si vos utilisateurs et ordinateurs dans Active Directory suivent un modèle géographique, vous pouvez entrer `Acme - South America`. Cette entrée ne doit pas nécessairement correspondre à des paramètres dans Active Directory, mais l'utilisation de modèles similaires dans les deux systèmes peut aider à organiser vos terminaux dans vos jonctions de domaine.
4. Sélectionnez **Groupe de travail** dans **Type de jonction de domaine**.
5. Entrez le nom pour le **Groupe de travail**. Le nom vous permet d'organiser et d'identifier le groupe de travail dans la console Workspace ONE UEM.
6. Entrez le format du nom pour la machine dans le champ **Format du nom de la machine**. Utilisez un format pris en charge pour le nom de votre machine. L'infobulle spécifie les formats pris en charge dans l'interface utilisateur. Utilisez exactement 15 caractères au format `%SERIAL%` ou `%RAND:[#]%`.
7. Si vous voulez créer directement l'utilisateur local pour la jonction de domaine, activez **Créer un utilisateur local**.
8. Si vous souhaitez accorder à l'utilisateur local des autorisations d'admin, activez **Définir en tant qu'administrateur**. Les administrateurs ont des autorisations qui incluent la possibilité de désenrôler les terminaux ou de désinstaller les applications système.
9. Entrez un **Nom d'utilisateur local** et un **Mot de passe d'utilisateur local** que l'utilisateur du terminal pourra entrer pour accéder au terminal avec cette configuration de jonction de domaine. Renseignez une entrée pour le nom d'utilisateur et le mot de passe de vos utilisateurs.
10. Enregistrez la configuration de jonction de domaine pour l'attribuer ultérieurement ou sélectionnez **Enregistrer et attribuer** maintenant.

Deuxième étape : Attribuer une configuration de jonction de domaine

1. Dans Workspace ONE UEM console, accédez à une page d'attribution en sélectionnant **Attribuer** dans l'affichage en liste de la jonction de domaine dans **Groupes et paramètres > Configurations** et sélectionnez **Jonction de domaine**. Cette fenêtre de configuration s'affiche si vous sélectionnez **Enregistrer et attribuer** pour votre configuration de jonction de domaine.
2. Sélectionnez le nom de la configuration de jonction de domaine, sauf si l'entrée est préremplie.
3. Ajoutez un **Nom de l'attribution** qui vous aidera à identifier l'attribution. L'entrée ne doit pas nécessairement correspondre à un paramètre dans Active Directory.
4. Recherchez et sélectionnez des Smart Groups configurés dans Workspace ONE UEM. Vous ne pouvez attribuer qu'une seule configuration de groupe de travail par Smart Group. Si vous essayez de sélectionner un Smart Group qui est déjà attribué à une configuration de groupe de travail, la console affiche un message d'erreur contenant des informations de dépannage, vous permettant ainsi de choisir quels Smart Groups utiliser pour répondre à votre scénario de déploiement actuel.
5. Créez et enregistrez votre attribution.

Intégration d'Intel vPro Endpoint Management Assistant (EMA) de disponibilité générale pour Windows on SaaS

Utilisez la nouvelle zone **Intégrations** de Workspace ONE UEM pour intégrer votre déploiement Intel vPro Endpoint Management Assistant (EMA) à Workspace ONE UEM. Intel EMA gère les terminaux Windows équipés d'un chipset Intel vPro. EM EMA utilise la technologie de gestion active Intel (AMT) pour accéder aux terminaux Windows qui ne répondent pas ou qui ont un système d'exploitation endommagé. Intégrez les systèmes afin de pouvoir enrôler de nouveaux terminaux avec Intel EMA et afficher vos terminaux gérés par Intel EMA et Workspace ONE UEM et gérer ces terminaux depuis une console unique.

Conditions prérequises

- Cette fonctionnalité n'est qu'une offre SaaS et n'est actuellement pas prise en charge sur site.
- Déployez un serveur Intel EMA avec les informations d'identification du client configurées pour le locataire.
- Obtenez les valeurs répertoriées à partir de votre environnement Intel EMA. Workspace ONE UEM utilise ces valeurs pour se connecter et communiquer avec Intel EMA.
    - URL de serveur
    - ID client
    - Client Secret
- Configurez vos groupes de points de terminaison dans Intel EMA avant de démarrer cette intégration.
- Téléchargez l'outil de configuration de point de terminaison Intel et configurez-le pour le déployer sur tous les terminaux cogérés.

L'ID client et la clé secrète client doivent être configurés dans Intel EMA à l'aide du processus de génération d'identification client pour l'authentification système à système. Veuillez suivre la documentation officielle d'Intel à l’adresse https://www.intel.com/content/www/us/en/support/articles/000090097/software/manageability-products.html Téléchargez l'ECT Intel officiel : https://intel.com/content/www/us/en/download/19805/intel-endpoint-management-assistant-configuration-tool-intel-ema-configuration-tool.html

Configurer l'intégration Intel EMA

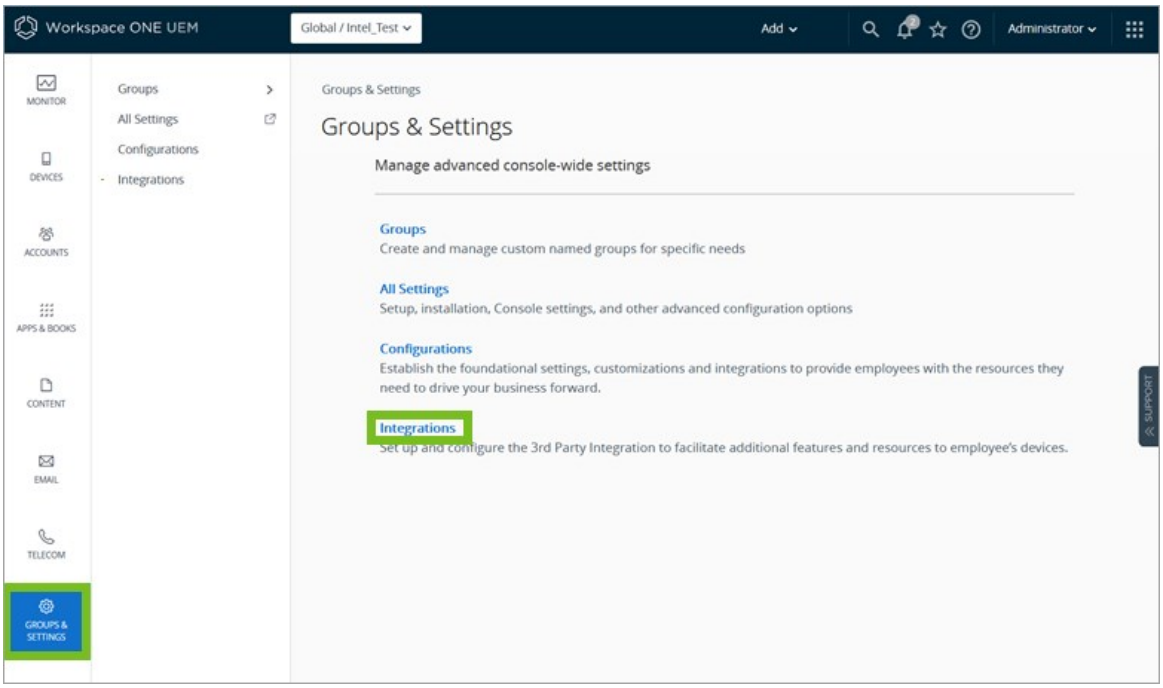
Entrez votre serveur Intel EMA et les informations d'identification dans Workspace ONE UEM afin que les systèmes puissent communiquer. Workspace ONE UEM détecte vos terminaux enrôlés Intel EMA et les répertorie dans l'affichage en liste des terminaux Workspace ONE UEM. Les terminaux cogérés obtiennent des balises générées par le système (Intel EMA et le nom du groupe de points de terminaison) afin faciliter le regroupement et les actions. Workspace One UEM crée également des modules d'applications pour les groupes de points de terminaison Intel EMA. Ces modules d'applications contiennent l'agent Intel EMA ainsi que la configuration et peuvent être déployés sur de nouveaux points de terminaison à l'aide du flux de déploiement d'applications.

Déploiement de la configuration des groupes de points de terminaison Intel EMA et de l'agent à l'aide des déploiements d'applications UEM

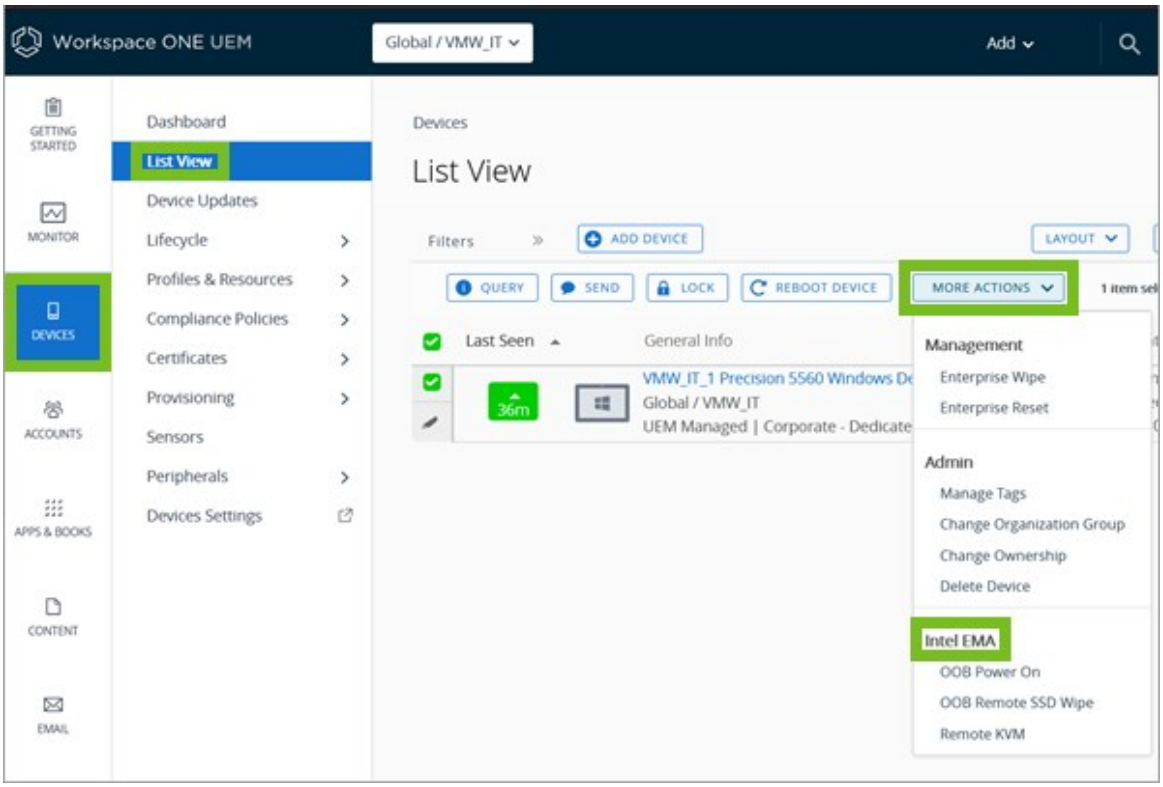
Cette rubrique inclut des informations générales sur l'utilisation d'une attribution d'application pour déployer vos modules Intel EMA, groupes de points de terminaison dans Workspace ONE UEM. Les groupes de points de terminaison Intel EMA sont mis à disposition sous forme d'applications natives. Pour plus d'informations sur les attributions d'applications, accédez Ajouter des attributions et des exclusions à vos applications.

Procédure

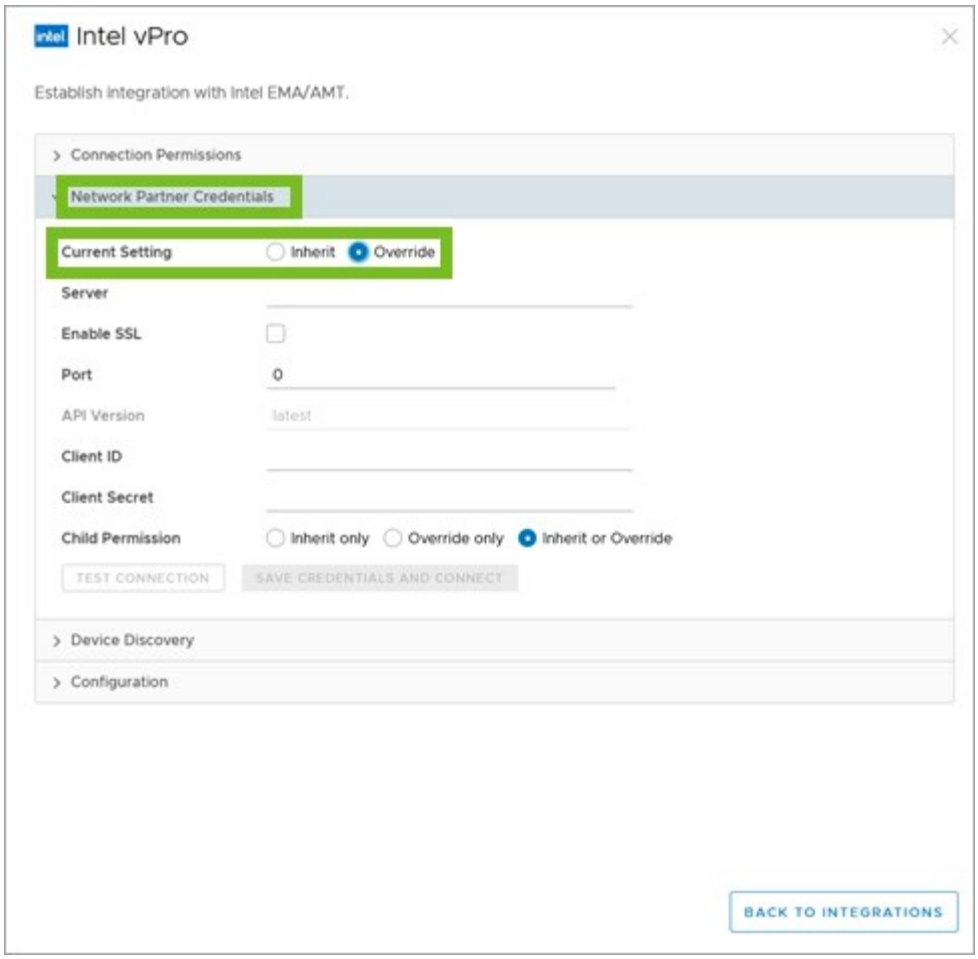
1. Workspace ONE UEM sélectionnez le groupe organisationnel applicable.
2. Accédez à **Groupes et paramètres > Intégrations**.



3. Sélectionnez **Configurer** sur la carte **Intel** pour configurer l'intégration.



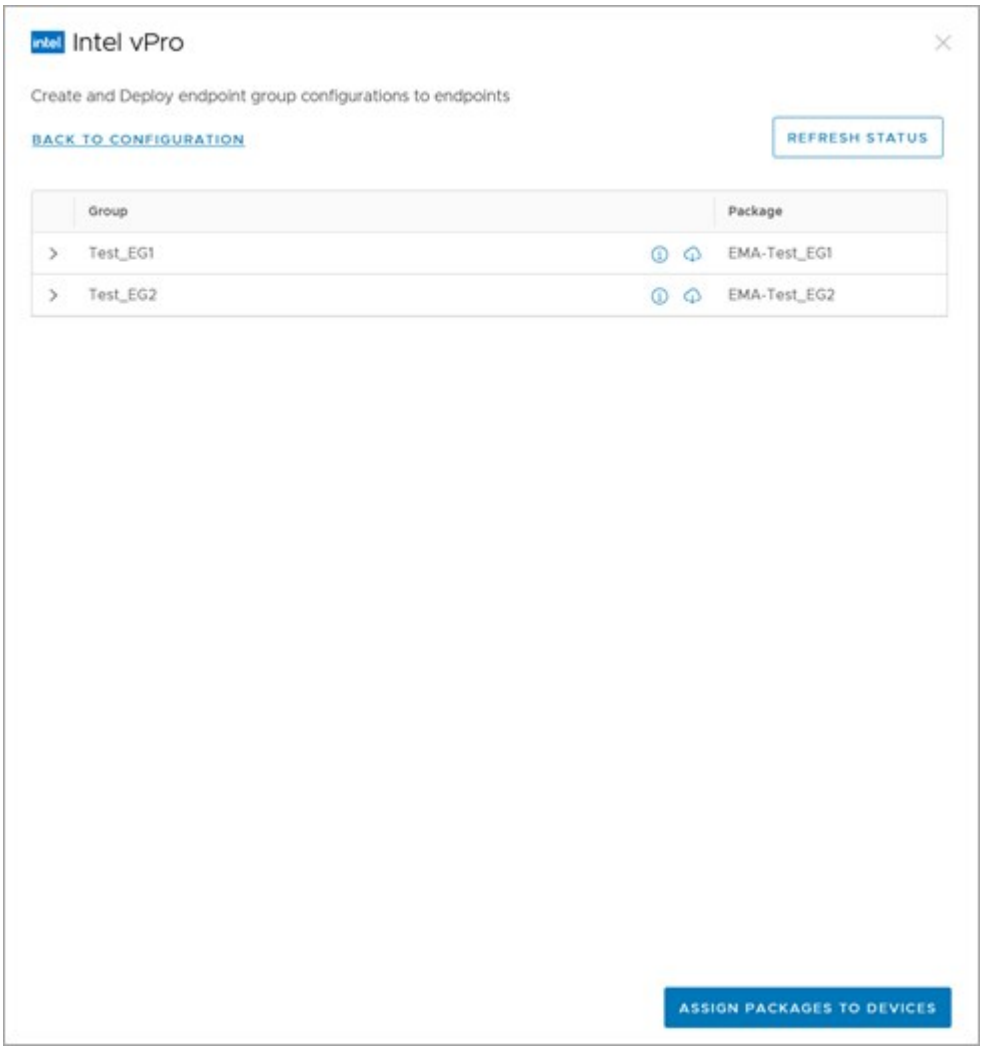
4. Sélectionnez l'onglet **Informations d'identification du partenaire réseau** et affichez ou modifiez le **Paramètre Actuel**.
    - **Hériter** configure le système afin qu'il utilise les paramètres du groupe organisationnel parent du groupe organisationnel actuel.
    - **Remplacer** active les paramètres à modifier afin que vous puissiez modifier directement les paramètres du groupe organisationnel actuel.



5. Ajoutez vos valeurs Intel EMA aux éléments de menu **Server**, **Client ID** et **Client Secret**.
6. Sélectionnez le bouton **Tester la connexion** pour vérifier que les systèmes communiquent.
7. Sélectionnez cette option pour **Enregistrer les informations d'identification et connecter**. Cette action démarre plusieurs processus.
    1. Workspace ONE UEM lance un processus de détection de terminaux.
        - Le processus de détection des terminaux trouve les terminaux qui étaient déjà gérés dans Workspace ONE UEM et dans Intel EMA avant l'intégration.
        - Vous pouvez relancer ce processus dans l'onglet **Détection des terminaux** de la carte Intégrations **Intel**.
    2. Workspace ONE UEM communique avec le serveur Intel EMA.
        - Workspace ONE UEM récupère les détails de tous les groupes de points de terminaison configurés sur le serveur.
        - Vous pouvez resynchroniser des groupes de points de terminaison dans l'onglet **Configuration** de la carte Intégrations **Intel**.
8. Dans l'onglet **Configuration**, vous pouvez voir une vue de liste des groupes de points de terminaison Intel EMA découverts.
    - Affichez les détails Intel EMA et Intel AMT du module Groupe de points de terminaison.
    - Affichez la date de la dernière création du groupe de points de terminaison.

- Téléchargez les groupes de points de terminaison si vous en avez besoin.

9. Dans l'onglet **Configuration**, sélectionnez **Attribuer des modules aux terminaux**. Cette action vous dirige vers le flux d'attribution d'application dans Workspace ONE UEM.

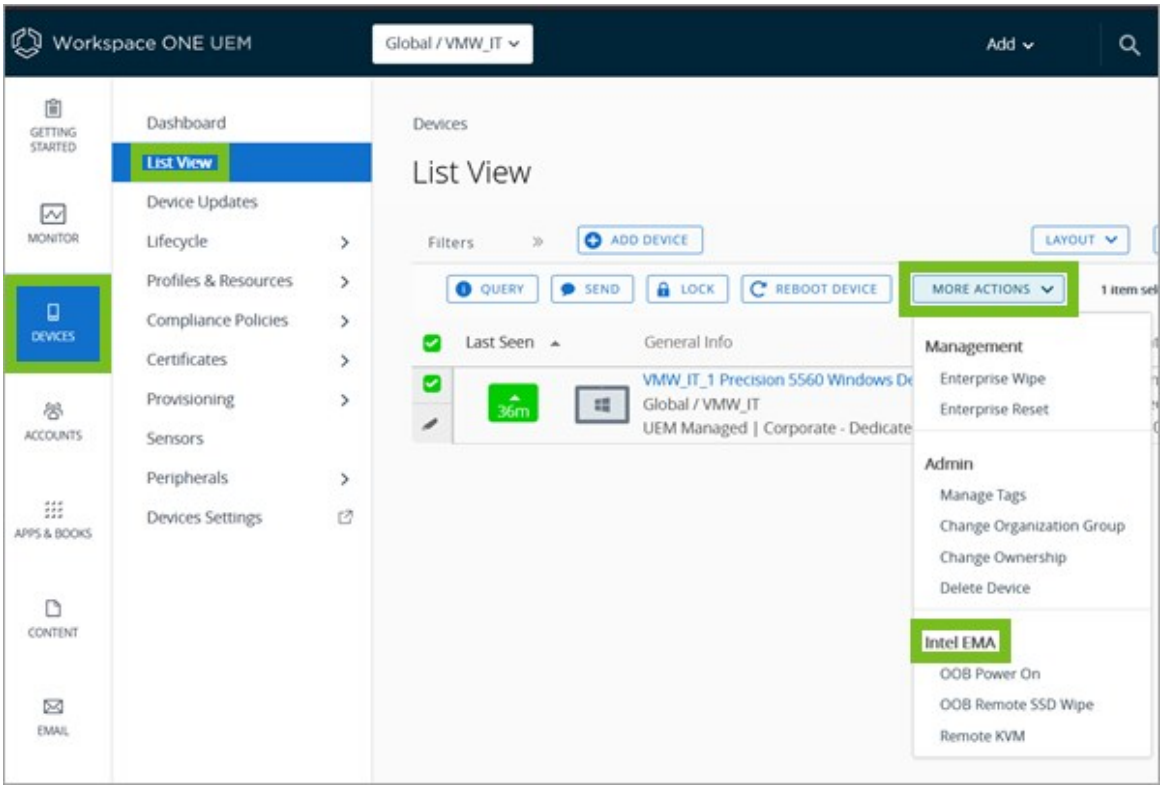


10. Le système accède à la page d'affichage en liste des applications dans laquelle vous voyez vos modules de groupe de points de terminaison. L'affichage en liste des applications se trouve dans la console à l'adresse **Ressources > Applications > Natives > Internes**.
11. Sélectionnez le bouton radio de l'un des modules **EMA** Groupe de points de terminaison, puis sélectionnez **Attribuer**. Vous pouvez utiliser la zone de texte **Rechercher la liste** pour rechercher un groupe spécifique.
12. Sélectionnez **Ajouter une attribution**.
    Vous pouvez également modifier une attribution d'application existante.
13. Dans l'onglet **Distribution**, configurez les champs requis et sélectionnez des Smart Groups de terminaux dans l'élément de menu **Groupes d'attribution** pour déployer ces modules de groupe de points de terminaison sur les terminaux.
14. Sélectionnez **Créer** ou **Enregistrer** pour enregistrer l'attribution d'application pour le module Groupe de points de terminaison.

Rechercher les détails du module de groupe de points de terminaison dans la console

Workspace ONE UEM répertorie les détails du module Groupe de points de terminaison dans l'**Affichage en liste des terminaux**.

1. Dans la console Workspace ONE UEM, accédez à **Terminaux > Affichage en liste** pour voir vos terminaux Intel EMA enrôlés.



2. Examinez la colonne **Balises** des balises répertoriées. Ces balises identifient vos terminaux enrôlés Intel EMA détectés par Workspace ONE UEM.
    - Intel EMA
    - Groupe de points de terminaison Intel EMA

Exécuter les opérations gérées par Intel EMA sur les terminaux gérés depuis la console

Conditions prérequises

Tous les terminaux qui doivent être cogérés par Workspace ONE UEM et Intel EMA/AMT doivent répondre aux conditions répertoriées.

- Les terminaux doivent utiliser la puce Intel VPro.
- Les terminaux doivent disposer du microprogramme Intel AMT, version 11 ou ultérieure.
- Les terminaux déjà enrôlés doivent disposer du microprogramme Intel AMT et de l'agent Intel EMA correctement configurés.
- L'outil de configuration de point de terminaison Intel (ECT, Endpoint Configuration Tool) doit être déployé sur tous les terminaux. Vous pouvez le déployer à l'aide du flux de

déploiement de l'application Workspace ONE UEM. Ce dernier permet la collecte et l'exécution de terminaux des opérations Intel EMA/AMT sur les terminaux.

Procédure

Dans l'**Affichage en liste des terminaux**, sélectionnez un ou plusieurs terminaux Intel EMA enrôlés pour afficher et utiliser les opérations répertoriées dans le menu **Plus d'actions**. La sélection de périphériques détermine la disponibilité des opérations Intel EMA. La console répertorie les opérations disponibles en fonction de la définition du groupe de points de terminaison du terminal et de ses capacités. En outre, les capacités du terminal peuvent être affectées par les paramètres du BIOS/microprogramme.

Dans le menu **Plus d'actions** recherchez les opérations répertoriées.

- Mettre sous tension OOB
- Mettre hors tension OOB
- Cycle d'alimentation matérielle OOB
- Veille OOB - Liaison
- Veille OOB - En profondeur
- Effacement SSD distant OOB
- KVM distant

Comportements des opérations Intel EMA

- Les opérations Intel EMA se comportent de la même manière que d'autres actions de terminal Workspace ONE UEM.
- Vous pouvez déployer la plupart de ces opérations sur plusieurs terminaux à l'exception des opérations **Effacement SSD distant OOB** et **Supprimer KVM**. Vous ne pouvez déployer ces opérations que sur des terminaux uniques.
- L'effacement SSD distant OOB est disponible sur un nombre limité de terminaux/SSD pris en charge (Intel, Lenovo). Il dépend également des paramètres OEM.
- Lorsque vous sélectionnez l'opération **Remote KVM**, cette action vous dirige vers le portail Intel EMA. À partir de ce portail, vous pouvez vous connecter à distance au terminal.

Liens officiels de téléchargement Intel

Comme indiqué ci-dessus, le logiciel Intel est une condition préalable pour l'intégration intel vPro. Si vous devez toujours télécharger le logiciel, consultez les sites suivants : - Pour télécharger l'EMA Intel officiel : https://intel.com/content/www/us/en/download/19449/intel-endpoint-management-assistant-intel-ema.html - Pour télécharger l'ECT Intel officiel : https://intel.com/content/www/us/en/download/19805/intel-endpoint-management-assistant-configuration-tool-intel-ema-configuration-tool.html