Gestion de terminaux Windows Desktop

VMware Workspace ONE UEM

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

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

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

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

Table des matières

Gestion des terminaux Workspace ONE UEM pour les terminaux Windows Desktop

1

Workspace ONE UEM powered by AirWatch fournit un ensemble de solutions de gestion de la mobilité fiables pour enrôler, sécuriser, configurer et gérer les déploiements de terminaux Windows 10. En savoir plus sur la façon dont Workspace ONE UEM active la gestion des terminaux Windows 10.

Dans Workspace ONE UEM Console, vous pouvez utiliser plusieurs outils et fonctionnalités pour gérer le cycle de vie des terminaux personnels des collaborateurs ou des terminaux professionnels. 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 les terminaux personnels des collaborateurs, mais aussi les terminaux professionnels afin de sécuriser les données et le contenu de votre 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.

Enrôler vos terminaux dans Workspace ONE UEM vous permet de sécuriser et configurer les terminaux selon vos besoins.

Ce chapitre contient les rubriques suivantes :

Conditions d'inscription requises pour les terminaux Windows Desktop

Avant d'inscrire vos terminaux Windows Desktop (Windows 10) avec Workspace ONE UEM, vos utilisateurs finaux doivent répondre aux exigences et configurations répertoriées, autrement l'inscription ne fonctionne pas.

- **Environnement actif** : votre environnement Workspace ONE UEM actif et votre accès à Workspace ONE UEM Console.

- **Autorisations administrateur appropriées** : type d'autorisation qui vous permet de créer des profils, de déterminer des politiques et de gérer les terminaux dans Workspace ONE UEM Console.
- **Exécution de PowerShell** – La gestion de Workspace ONE UEM des terminaux Windows Desktop utilise PowerShell pour les modifications opérationnelles et d'installation via Workspace ONE Intelligent Hub.
- **URL d'enrôlement** – URL propre à l'environnement d'enrôlement ; vous dirige directement vers l'écran d'enrôlement. Par exemple : **mdm.example.com**.
- **ID de groupe** : l'ID de groupe associe votre terminal à votre rôle au sein de l'entreprise et est défini dans Workspace ONE UEM Console.
- **Certificat racine du terminal** : vous devez configurer le certificat racine du terminal dans les paramètres système avant d'enrôler des terminaux. Pour configurer le certificat, accédez à **Groupes et paramètres > Tous les paramètres > Système > Avancé > Certificat racine du terminal**.

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.

Quelles sont les versions de Windows 10 prises en charge ?

Workspace ONE UEM powered by AirWatch prend en charge l'enrôlement et la gestion des terminaux Windows 10. Le niveau de prise en charge dépend de la version du système d'exploitation et de l'architecture du terminal.

Plateformes et terminaux supportés

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

- Windows 10 Pro
- Windows 10 Entreprise
- Windows 10 Éducation
- Windows 10 Famille
- Windows 10 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 10 : https://technet.microsoft.com/en-us/windows/release-info.aspx.

Matrice de la version de Windows 10

Comparez la fonctionnalité MDM dans chaque version du système d'exploitation Windows 10. Workspace ONE UEM prend en charge toutes les versions du système d'exploitation Windows 10, ainsi que les fonctions prises en charge.

Les différentes éditions de Windows 10 (Famille, Professionnel, Entreprise et Éducation) sont dotées de fonctionnalités différentes. L'édition Windows 10 Famille ne prend pas en charge les fonctionnalités avancées disponibles dans le système d'exploitation Windows 10. Envisagez d'utiliser les éditions Entreprise ou Éducation pour bénéficier de la plupart des fonctionnalités.

Fonctionnalité	Windows 10 Famille	Windows 10 Professionnel	Windows 10 Entreprise	Windows 10 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	✓	✓	✓	✓

Fonctionnalité	Windows 10 Famille	Windows 10 Professionnel	Windows 10 Entreprise	Windows 10 Éducation
Effacement des données professionnelles	✓	✓	✓	✓
Réinitialisation complète du terminal	✓	✓	✓	✓
E-mail et Exchange ActiveSync	✓	✓	✓	✓
Wi-Fi	✓	✓	✓	✓
VPN	✓	✓	✓	✓
Gestion des certificats	✓	✓	✓	✓
Restrictions et gestion du terminal	✓	✓	✓	✓
Windows Hello	✓	✓	✓	✓
Personnalisation			✓	✓
Chiffrement	✓3	✓	✓	✓
Contrôle des applications (AppLocker)			✓	✓
Attestation d'intégrité	✓	✓	✓	✓
Windows Update for Business		✓	✓	✓
Accès attribué			✓	✓
Gestion d'applications		✓	✓	✓
Workspace ONE Content	✓	✓	✓	✓
Suivi des actifs		✓	✓	✓
Statut des terminaux		✓	✓	✓
Adresse IP				
Emplacement	✓	✓	✓	✓

Fonctionnalité	Windows 10 Famille	Windows 10 Professionnel	Windows 10 Entreprise	Windows 10 Éducation
Sécurité		✓	✓	✓
Envoi de messages au support technique (E-mails et SMS uniquement)		✓	✓	✓

1 – L'édition Entreprise comprend également IoT et LTSB (Long-Term Servicing Branch). L'édition LTSB est une image distincte de Windows 10 Entreprise comportant de nombreuses applications natives, y compris MicrosoftEdge, Cortana ; quant au Microsoft Store, il est supprimé. Certaines fonctionnalités de Workspace ONE UEM qui exploitent ces fonctions ne seront pas prises en charge.

2 – Microsoft Passport requiert une protection matérielle des identifiants/clés TPM 1.2 ou 2.0 ; si aucun TPM n'existe ou n'est configuré, la protection des identifiants et des clés sera basée sur le système d'exploitation.

3 – Le chiffrement du terminal pour la version Famille n'inclut pas le chiffrement BitLocker.

4 – Peut être téléchargé uniquement depuis le Microsoft Store. Windows 10 Famille ne prend pas en charge l'envoi d'applications internes par push.

5 – Requiert le téléchargement de Workspace ONE Intelligent Hub depuis le Microsoft Store.

Enrôlement de terminaux Windows 10 dans Workspace ONE UEM

2

Workspace ONE UEM prend en charge plusieurs méthodes pour enrôler vos terminaux Windows 10. 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 de terminal.

Notions de base relatives à l'enrôlement

Avant d'enrôler des terminaux, veillez à disposer des informations d'enrôlement adéquates. Consultez Conditions d'inscription requises pour les terminaux Windows Desktop pour plus d'informations.

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 utilisent la fonctionnalité native MDM du système d'exploitation Windows, Workspace ONE Intelligent Hub pour Windows ou l'intégration d'Azure AD.

Si vous souhaitez utiliser Workspace ONE UEM pour gérer les terminaux Windows gérés par SCCM, vous devez télécharger le client d'intégration VMware AirWatch SCCM. Utilisez ce client pour enrôler des terminaux gérés par SCCM dans Workspace ONE UEM.

Workspace ONE Intelligent Hub pour l'enrôlement Windows

Le workflow d'enrôlement le plus simple consiste à utiliser Workspace ONE Intelligent Hub pour Windows afin d'enrôler des terminaux. Il suffit aux utilisateurs finaux de télécharger Workspace ONE Intelligent Hub sur awagent.com et de suivre les invites d'enrôlement.

Pensez à utiliser le workflow d'enrôlement Workspace ONE Intelligent Hub pour 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 via l'intégration d'Azure AD prend en charge trois processus d'enrôlement différents : jonction à Azure AD, enrôlement en mode OOBE et enrôlement via 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 10 avant de le livrer à votre utilisateur final, il est conseillé d'utiliser le préenrôlement via Windows Desktop. Ce workflow d'enrôlement vous permet 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 10.

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 10 Provisioning Service by VMware AirWatch s'applique uniquement aux terminaux Dell Enterprise dotés de l'image Windows 10 appropriée. 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 10, 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.

Ce chapitre contient les rubriques suivantes :

Workspace ONE Intelligent Hub pour l'enrôlement Windows 10

Workspace ONE Intelligent Hub fournit une ressource unique pour l'enrôlement et facilite la communication entre le terminal et l'utilisation de Workspace ONE Intelligent Hub Workspace ONE UEM Console pour simplifier l'enrôlement et activer la fonctionnalité MDM complète.

Vous pouvez utiliser Workspace ONE Intelligent Hub pour Windows pour enrôler vos terminaux Windows Desktop, car il fournit le flux d'enrôlement le plus simple pour les utilisateurs. Si vous avez configuré Workspace ONE, le téléchargement de Workspace ONE Intelligent Hub à partir de https://getwsone.com/ entraîne également le téléchargement de l'application Workspace ONE. Lorsque vous terminez l'enrôlement avec Workspace ONE Intelligent Hub, l'application Workspace ONE se lance automatiquement et se configure 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

AirWatch Cloud Messaging (AWCM) permet de distribuer en temps réel des stratégies et des commandes sur Workspace ONE Intelligent Hub. Sans AWCM, Workspace ONE Intelligent Hub reçoit uniquement une distribution de stratégies et de commandes lors des intervalles de vérification normaux définis dans Workspace ONE UEM Console. Envisagez d'utiliser AWCM pour distribuer en temps réel des politiques et des commandes aux terminaux Windows Desktop.

Enrôler avec VMware Workspace ONE Intelligent Hub

Utilisez Workspace ONE Intelligent Hub pour enrôler vos terminaux Windows 10. Workspace ONE Intelligent Hub fournit aux utilisateurs un flux d'enrôlement simple et rapide.

Procédure

1. Accédez à https://getwsone.com sur le terminal Windows Desktop.
2. Installez 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 Windows Auto-Discovery, définissez les paramètres suivants :
   a. Saisissez l'**URL du serveur** et sélectionnez **Suivant**.
   b. Saisissez l'**ID de groupe** et sélectionnez **Suivant**.
   c. 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 effectuez 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.

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 Workspace ONE Intelligent Hub pour enrôler les terminaux Windows 10 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 lot pour les terminaux Windows 10.

Le service Windows Auto-Discovery simplifie l'enrôlement pour les utilisateurs en réduisant leur interaction nécessaire lors du processus. L'utilisation du service Windows Auto-Discovery nécessite de suivre la procédure décrite dans le **Guide d'installation du service VMware AirWatch Windows Auto-Discovery**.

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 10. L'enrôlement par Work Access et avec Windows Auto Discovery fournit aux utilisateurs un flux d'enrôlement simple et rapide.

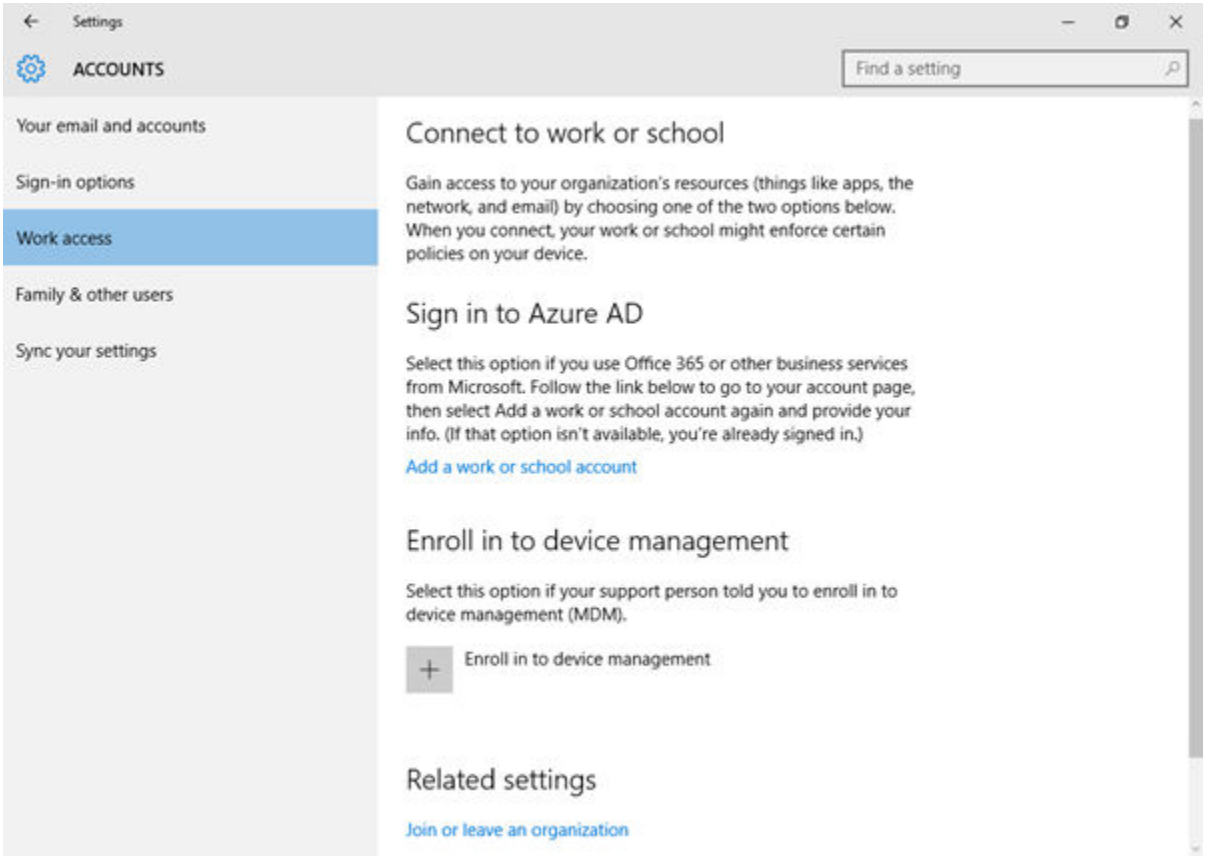
Conditions préalables

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

Note vous pouvez utiliser Workspace ONE Intelligent Hub pour Windows pour enrôler vos terminaux Windows 10 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, naviguez vers **Paramètres > Comptes > Accès professionnel** et sélectionnez **Enrôler dans la gestion des terminaux**.



2 Saisissez le nom d'utilisateur fourni à votre utilisateur dans la zone de texte **E-mail**, suivi du domaine de l'environnement au format NomUtilisateur@domaine.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**.

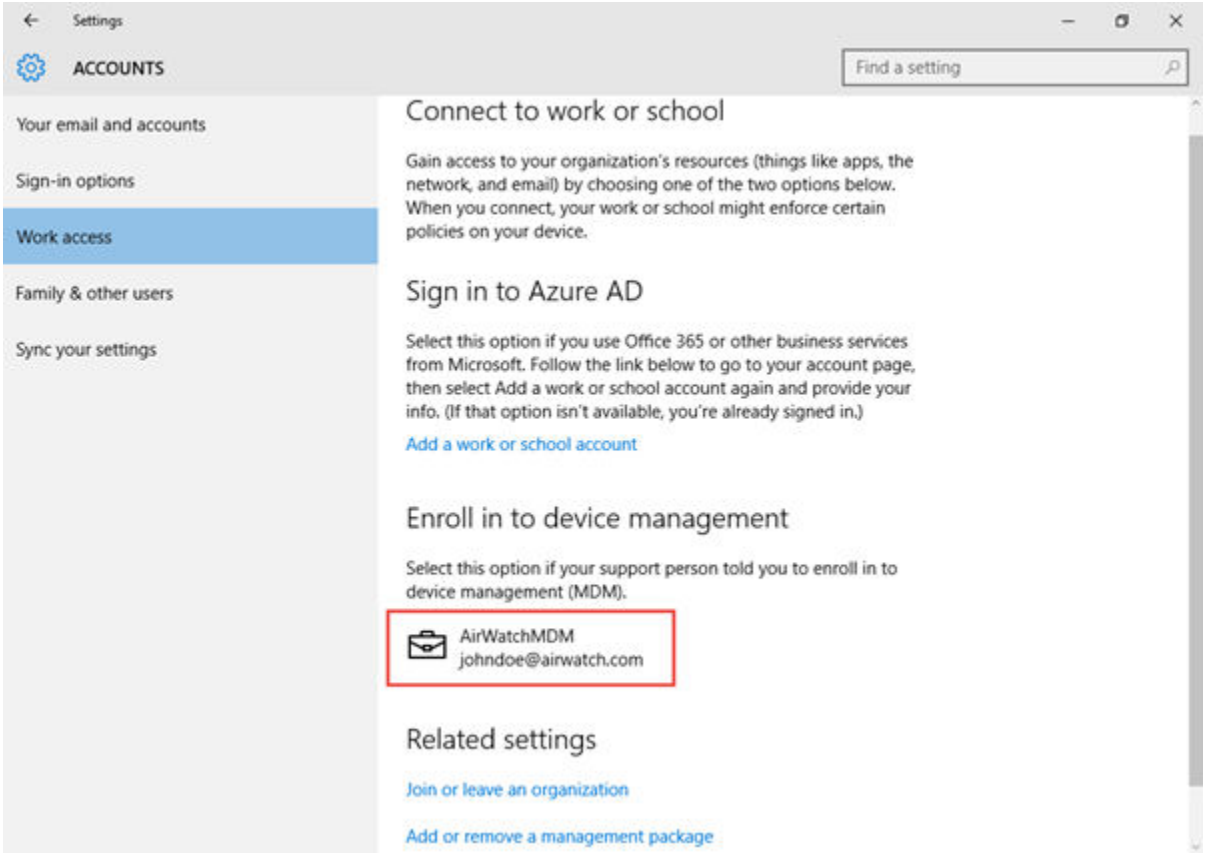
Il peut s'agir de vos identifiants de services d'annuaire ou d'identifiants dédiés propres à votre environnement Workspace ONE UEM.

5 (Facultatif) Lisez le Contrat de licence d'utilisateur final et sélectionnez **J'accepte** pour accepter les conditions d'utilisation.

L'étape suivante est facultative et n'apparaît que si vous l'avez activée dans Workspace ONE UEM Console.

6 (Facultatif) Sélectionnez **Oui** pour enregistrer vos informations de connexion.

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

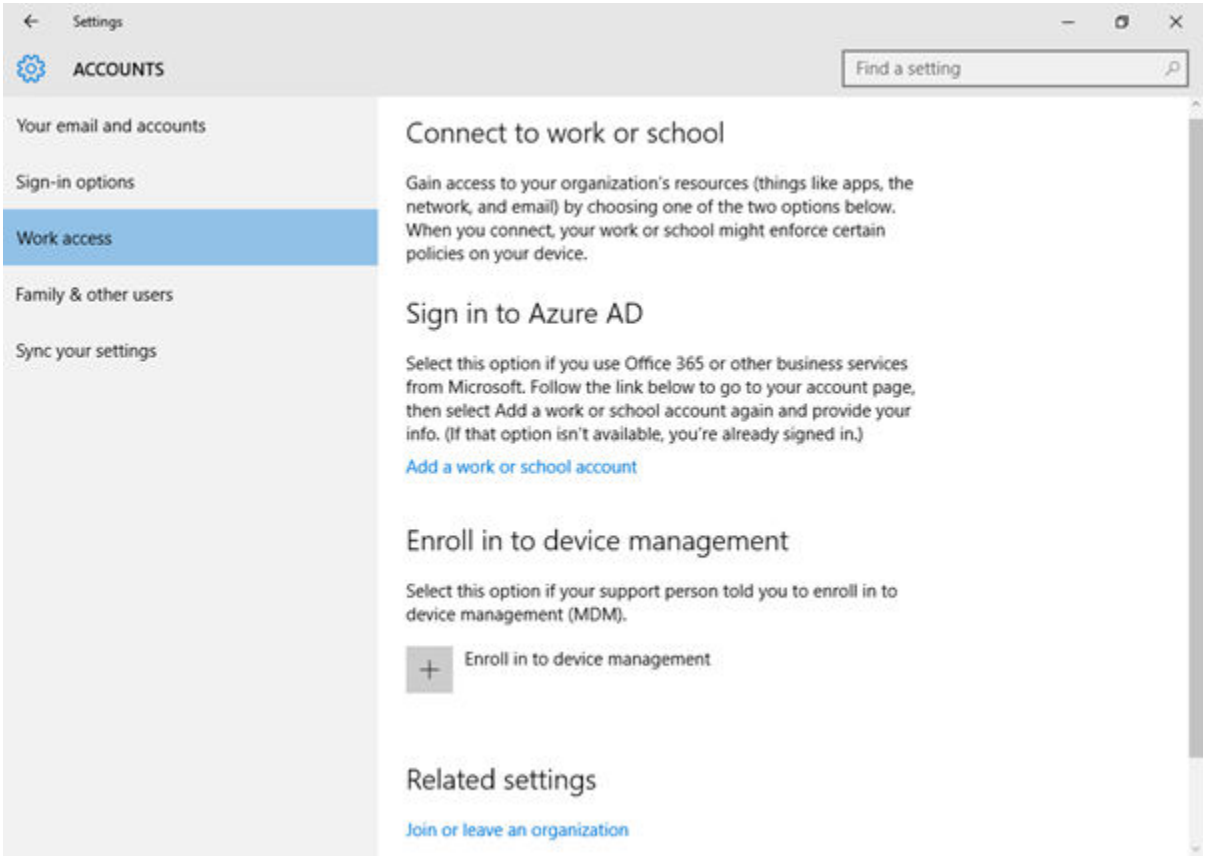
Work Access est la méthode d'enrôlement MDM native pour les terminaux Windows 10. L'enrôlement via Work Access sans WADS nécessite la saisie manuelle des identifiants de l'utilisateur.

Conditions préalables

Note vous pouvez utiliser Workspace ONE Intelligent Hub pour Windows pour enrôler vos terminaux Windows 10 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, naviguez vers **Paramètres > Comptes > Accès professionnel** et sélectionnez **Enrôler dans la gestion des terminaux**.



2 Saisissez le nom d'utilisateur fourni à votre utilisateur dans la zone de texte **E-mail**, suivi du domaine de l'environnement au format NomUtilisateur@domaine.com (par exemple, jdoe1@acme.com).

3 **Saisissez l'adresse du serveur** comme suit : <URLServicesTerminal>/DeviceServices/Discovery.aws. N'incluez pas « https:// » dans l'URL.

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**.

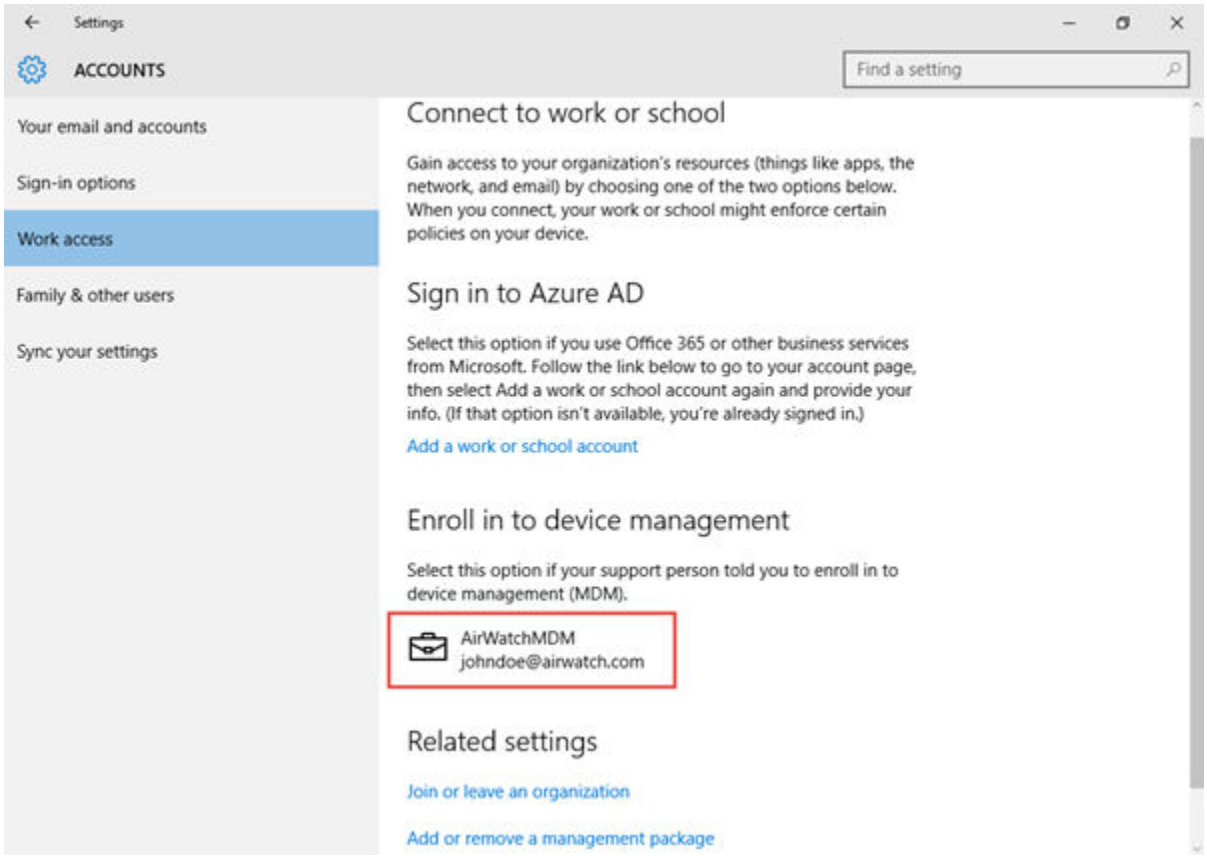
Il peut s'agir de vos identifiants de services d'annuaire ou d'identifiants dédiés propres à votre environnement Workspace ONE UEM.

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.

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 du terminal Windows 10

Avec la fonction de préenrôlement des terminaux, vous pouvez configurer vos terminaux Windows 10 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.

La préinscription des terminaux vous permet d'inscrire votre terminal Windows 10 dans Workspace ONE UEM. Cette inscription requiert le démarrage de Workspace ONE Intelligent Hub. 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 la 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** – Importez et installez Workspace ONE Intelligent Hub et saisissez les identifiants d'enrôlement. Pour cette méthode, les terminaux doivent être joints au domaine avant leur enrôlement.
- **Installation par ligne de commande** – Importez Workspace ONE Intelligent Hub, puis installez et enrôler 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 > Statut d'enrôlement**.
   a. Sélectionnez **Ajouter**, puis **Importation par lots** pour afficher l'écran **Importation par lots**.
2. Renseignez chacune des options obligatoires. **Nom du lot**, **Description du lot** et **Type de lot**.
3. 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.
4. Sélectionnez le modèle de téléchargement approprié et enregistrez le fichier de valeurs séparées par des virgules (CSV, comma-separated values) dans un emplacement accessible.
5. 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.
6. 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.
7. Cliquez sur **Enregistrer** pour terminer l'inscription pour tous les utilisateurs listés et les terminaux correspondants.

Enrôlement par préenrôlement à 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 enrôle le terminal et télécharge les profils de niveau terminal en fonction des identifiants utilisateur entrés.

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.

Note Ce produit ne doit pas être utilisé pour une installation silencieuse de VMware Workspace ONE Intelligent Hub pour Windows sur les terminaux personnels (BYOD). Si vous effectuez une installation silencieuse sur des terminaux personnels (BYOD), vous êtes tenu d'informer les utilisateurs finaux de votre terminal sur l'utilisation de l'installation silencieuse et des données collectées à partir des applications installées en silence, et d'obtenir tout consentement légal requis ou de respecter les lois applicables.

Procédure

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

   Télécharge 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 du dossier de téléchargement vers un dossier du disque local ou d'un lecteur réseau.

2. Ouvrez une ligne de commande ou créez un fichier BAT, puis saisissez les chemins d'accès, paramètres et valeurs nécessaires en utilisant les informations de Paramètres et valeurs de l'enrôlement silencieux.

3. Exécutez la commande. Pour des exemples de syntaxe, reportez-vous à Paramètres et valeurs de l'enrôlement silencieux.

   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 10 à l'aide de 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 préalables

Ces terminaux doivent être intégrés à un domaine.

Procédure

1. Naviguez vers www.awagent.com pour télécharger le programme d'installation de 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 AirWatch Auto-Discovery est activée ; sinon, sélectionnez **Détails du serveur**.
5. Définissez les paramètres requis en fonction du type d'authentification sélectionné :
   a. Saisissez l'adresse e-mail pour remplir automatiquement l'écran des détails du serveur. Sélectionnez **Suivant** ; les détails sont entrés.
   b. Saisissez le nom du serveur et l'ID de groupe si vous n'utilisez pas AirWatch Auto-Discovery 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.

   Lorsque Workspace ONE Intelligent Hub détecte un utilisateur de préenrôlement, le module d'écoute de Workspace ONE Intelligent Hub s'exécute et écoute la connexion Windows suivante. Lorsque l'utilisateur se connecte au terminal, le module d'écoute de Workspace ONE Intelligent Hub lit l'UPN et l'adresse e-mail de l'utilisateur dans le 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 Workspace ONE Intelligent Hub se télécharge et s'installe sur les terminaux Windows 10.

Note N'utilisez pas ce produit pour installer Workspace ONE Intelligent Hub pour Windows en mode silencieux sur les terminaux personnels (BYOD). Si vous effectuez une installation silencieuse sur des terminaux personnels (BYOD), vous êtes tenu d'informer les utilisateurs finaux de votre terminal sur l'utilisation de l'installation silencieuse et des données collectées à partir des applications installées en silence, et d'obtenir tout consentement légal requis ou de respecter 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.

Tableau 2-1. Paramètres généraux

Paramètres d'enrôlement	Valeur à ajouter au paramètre
Tous les paramètres MSI	Ces paramètres contrôlent le comportement d'installation des applications. Cette liste contient des exemples. ■ **/quiet** : complètement silencieux ■ **/q** : contrôle les niveaux d'interface utilisateur pour l'installation ■ **/passive** : contrôles minimaux de l'utilisateur sur l'application ■ **/L** : niveaux de journalisation et chemins des journaux 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 du domaine qui est connecté.
DEVICEOWNERSHIPTYPE*	Sélectionnez **CD** pour Entreprise dédiée. Sélectionnez **CS** pour Entreprise partagée. Sélectionnez **EO** pour Employé propriétaire. Sélectionnez **N** pour Aucun.
DOWNLOADWSBUNDLE	Ce paramètre contrôle le téléchargement de l'application Workspace ONE lors de l'enrôlement. Sélectionnez **Y** pour télécharger le programme d'installation de l'application Workspace ONE pendant l'installation du Workspace ONE Intelligent Hub. Si vous enrôlez un terminal à l'aide du Workspace ONE Intelligent Hub, l'installation de Workspace ONE n'est pas facultative. Si vous ne définissez pas DOWNLOADWSBUNDLE sur **Y**, le programme d'installation de l'application 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**.
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.

Tableau 2-1. Paramètres généraux (suite)

Paramètres d'enrôlement	Valeur à ajouter au paramètre
INSTALLDIR*	Saisissez le chemin d'accès au répertoire si vous souhaitez changer le chemin d'installation. **Note** Si ce paramètre n'est pas présent, Workspace ONE Intelligent Hub utilise le chemin d'accès 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 astérisque (*) sont facultatifs.

Tableau 2-2. Paramètres Enrôlement pour le compte d'un utilisateur

Paramètres d'enrôlement	Valeur à ajouter au paramètre
SECURITYTYPE	Workflow Enrôlement pour le compte d'un utilisateur uniquement : utilisez ce paramètre si un compte d'utilisateur est ajouté à la Workspace ONE UEM Console au cours du processus d'enrôlement. ■ Sélectionnez **D** pour l'**annuaire**. ■ Sélectionnez **B** pour l'**utilisateur de base**.
STAGEEMAIL*	Workflow Enrôlement pour le compte d'un utilisateur uniquement : saisissez l'adresse e-mail de l'utilisateur que vous enrôlez.
STAGEEMAILUSRNAME*	Workflow Enrôlement pour le compte d'un utilisateur uniquement : saisissez le nom d'utilisateur de messagerie de l'utilisateur que vous enrôlez.
STAGEPASSWORD	Workflow Enrôlement pour le compte d'un utilisateur uniquement : saisissez le mot de passe de l'utilisateur que vous enrôlez.
STAGEUSERNAME	Workflow Enrôlement pour le compte d'un utilisateur uniquement : entrez le nom d'utilisateur de l'utilisateur enrôlé.

Les éléments signalés par un astérisque (*) sont facultatifs.

Exemples d'enrôlement silencieux

Vous trouverez ci-dessous 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 Windows 10 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=locationgroupid 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=URLEntreprise.com LGName=idegroupeemplacement USERNAME=UsrTest PASSWORD=test

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

Voici un exemple de paramètre de 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=URLEntreprise.com LGName=idgroupeemplacement USERNAME=UsrTest PASSWORD=test

Paramètres et valeurs disponibles

L'extrait suivant est un exemple de syntaxe utilisant la plupart des paramètres et valeurs disponibles indiqués dans le tableau précédent.

<AirwatchAgent.msi>/quiet INSTALLDIR=\"<Chemin d'accès au répertoire>" ENROLL=<Y/N> IMAGE=<Y/N>SERVER=<URLEntreprise>LGNAME=<ID groupe emplacement>USERNAME=<Nom d'utilisateur>PASSWORD=<Nom d'utilisateur/mot de passe>STAGEUSERNAME=<Nom d'utilisateur de préenrôlement>SECURITYTYPE=<D/B>STAGEEMAILUSRNAME=<Enrôlement utilisateur>STAGEPASSWORD=<Mot de passe pour l'enrôlement utilisateur>STAGEEMAIL=<Adresse e-mail pour l'enrôlement utilisateur>DEVICEOWNERSHIPTYPE<CD/CS/EO/N>ASSIGNTOLOGGEDINUSER=<Y/N>

Windows 10 Provisioning Service by VMware AirWatch

Workspace ONE UEM prend en charge l'enrôlement automatique des terminaux Windows Desktop spécifiques achetés chez Dell. Windows 10 Provisioning Service by VMware AirWatch simplifie le processus d'enrôlement en enrôlant automatiquement les terminaux enregistrés après l'expérience immédiate.

Windows 10 Provisioning Service by VMware AirWatch ne s'applique qu'à certains terminaux Dell Enterprise dotés de l'image Windows 10 adéquate. La fonctionnalité d'enrôlement automatique doit être achetée dans le cadre de la commande d'achat chez Dell. Workspace ONE UEM prend uniquement en charge les SKU Windows 10 versions Pro, Enterprise et Education pour Cloud Provisioning.

Windows 10 Provisioning Service by VMware AirWatch consiste à faire correspondre des terminaux enregistrés et des utilisateurs et à enregistrer automatiquement le terminal après l'expérience immédiate. Lorsque l'utilisateur final se connecte au terminal, l'agent de provisionnement du terminal reçoit les applications et les profils affectés au terminal et à l'utilisateur. Cette fonctionnalité est similaire au programme d'inscription des appareils Apple.

Lorsque vous achetez vos terminaux Dell, Dell fournit à Workspace ONE UEM les détails des terminaux achetés. Pour utiliser l'enrôlement automatique, vous devez enregistrer les numéros de série de tous les terminaux achetés chez Dell. Workspace ONE UEM fait correspondre le numéro de série à ceux fournis par Dell pour l'utilisation avec la détection automatique AirWatch.

Vous devez enregistrer les terminaux avec un compte utilisateur avant de les envoyer aux utilisateurs finaux.

Pour une expérience d'enrôlement fluide, pensez à configurer la méthode d'authentification par jeton d'accès externe pour VMware Identity Manager. L'authentification par jeton d'accès externe permet à Workspace ONE UEM de s'ouvrir automatiquement et de distribuer des applications au terminal. Lorsque la fonction est activée, Workspace ONE UEM s'authentifie automatiquement et affiche l'état d'avancement de l'installation des applications et des politiques lors du premier lancement.

Important Les terminaux enrôlés via Windows 10 Provisioning Service by VMware AirWatch ne seront pas automatiquement réenrôlés en cas de réinitialisation sur les paramètres d'usine. Le Windows 10 Provisioning Service by VMware AirWatch fonctionne uniquement pour le premier enrôlement.

Configurer Windows 10 Provisioning

Configurez Windows 10 Provisioning Service by VMware AirWatch pour enrôler automatiquement les terminaux Dell Windows Desktop. L'enrôlement automatique compare les numéros de série à une liste fournie par Dell pour l'enrôlement des terminaux dans le cadre de l'expérience immédiate.

Conditions préalables

Achetez Windows 10 Provisioning Service by VMware AirWatch dans le cadre de votre commande Dell.

Procédure

1 Naviguez vers **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Windows > Windows Desktop > Enrôlement automatique**.

2 Configurez les paramètres de l'enrôlement automatique :

Paramètres	Description
Enrôlement automatique	Sélectionnez **Activer** pour utiliser Windows 10 Provisioning Service by VMware AirWatch.
Intervalle de synchronisation	Sélectionnez la durée entre les tentatives de synchronisation entre Workspace ONE Intelligent Hub et Workspace ONE UEM Console.
Appliquer les politiques avant de se connecter	Sélectionnez **Activer** pour appliquer les règles du terminal avant que l'utilisateur ne s'y connecte.
Durée maximale avant la connexion	Sélectionnez le nombre maximal de minutes qui peuvent s'écouler avant qu'un utilisateur ne se connecte après avoir terminé l'expérience immédiate.

3 Cliquez sur **Enregistrer**.

4 Enregistrez les numéros de série des terminaux dans Workspace ONE UEM. Requise uniquement pour les clients sur site, cette étape est effectuée pour les clients SaaS. Vérifiez qu'il existe des dossiers d'enregistrement des terminaux. Si ce n'est pas le cas, procédez comme suit. Il existe trois workflows pour l'enregistrement des terminaux :

   a Naviguez jusqu'à **Comptes > Utilisateurs > Ajouter > Ajouter un utilisateur**, puis ajoutez le compte utilisateur. Lorsque vous avez ajouté l'utilisateur, sélectionnez **Enregistrer et ajouter un terminal.** Puis terminez les réglages de l'option Ajouter un terminal. Vous devez définir la **Plateforme** sur **Windows Desktop**.

   b Naviguez vers **Comptes > Utilisateurs > Ajouter > Importation en lots**. Téléchargez et complétez le modèle CSV pour l'utilisateur et/ou le terminal. Téléchargez le CSV et sélectionnez **Importer.** Vous devez entrer **Windows Desktop** comme **Plateforme du terminal** lorsque vous complétez le modèle. Vous devez définir la **Plateforme** sur **Windows Desktop**.

   c Naviguez jusqu'à Cycle de vie des terminaux > Statut d'enrôlement > Ajouter > Enregistrer le terminal. Vous devez définir la **Plateforme** sur **Windows Desktop**.

Intégration de Workspace ONE UEM et Azure AD

Grâce à l'intégration avec Microsoft Azure Active Directory, vous pouvez enrôler automatiquement vos terminaux Windows 10 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 10.

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 d'entrer des informations dans vos déploiements Azure AD et Workspace ONE UEM pour faciliter la communication.

L'enrôlement via l'intégration d'Azure AD prend en charge trois processus d'enrôlement différents : jonction à Azure AD, enrôlement en mode OOBE et enrôlement via Office 365. Toutes les méthodes nécessitent la configuration de l'intégration d'Azure AD avec Workspace ONE UEM.

Important L'enrôlement via l'intégration d'Azure AD requiert Windows 10 et une licence Azure Active Directory Premium.

Configuration de Workspace ONE UEM pour utiliser Azure AD comme service d'identité

Avant d'utiliser Azure AD pour enrôler vos terminaux Windows, vous devez configurer Workspace ONE UEM afin qu'il utilise Azure AD en tant que service d'identité. L'activation d'Azure AD est un processus en deux étapes qui nécessite l'ajout à Azure des détails d'enrôlement dans MDM.

Conditions préalables

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 locataire où le service Active Directory (tel que LDAP) est configuré.

Important si vous définissez le **Paramètre actuel** sur **Remplacer** sur la page des paramètres système du service d'annuaire, les paramètres LDAP doivent être configurés et enregistrer avant d'activer Azure AD pour les services d'identité.

Procédure

1. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > Services d'annuaire**.
2. Activez **Utiliser Azure AD pour les services d'identité** sous les paramètres **Avancé**. Copiez l'**URL d'enrôlement MDM** et l'**URL des conditions d'utilisation MDM**, car vous devez les entrer dans Azure.
3. Connectez-vous au portail de gestion Azure avec votre compte Microsoft ou le compte organisationnel.
4. Sélectionnez votre répertoire et accédez à l'onglet **Mobilité (MDM et MAM)**.

5 Sélectionnez **Ajouter une application**, sélectionnez l'application **AirWatch by VMware**, puis cliquez sur **Ajouter**.

6 Sélectionnez l'application **AirWatch by VMware** que vous avez ajoutée pour modifier la valeur du champ **Portée de l'utilisateur GDR** en **Tout**.

7 Collez l'**URL des conditions d'utilisation MDM** à partir de Workspace ONE UEM Console dans la zone de texte **URL des conditions d'utilisation de GDR** dans Azure. Collez l'**URL d'enrôlement MDM** à partir de Workspace ONE UEM Console dans la zone de texte **URL de détection MDM** dans Azure.

8 Ajoutez une application sur site en sélectionnant **Ajouter une application > Application MDM sur site**, puis en cliquant sur **Ajouter**.

9 Sélectionnez à nouveau l'**application MDM sur site** et configurez l'application MDM sur site. Dans **Portée de l'utilisateur GDR**, indiquez **Tout** ou **Certain(e)s**, puis sélectionnez un groupe d'utilisateurs.

10 Entrez les URL Workspace ONE UEM Console vers l'**application MDM sur site** et enregistrez les paramètres.

- Collez l'**URL des conditions d'utilisation MDM** à partir de Workspace ONE UEM Console dans la zone de texte **URL des conditions d'utilisation de GDR** dans Azure.
- Collez l'**URL d'enrôlement MDM** à partir de Workspace ONE UEM Console dans la zone de texte **URL de détection MDM** dans Azure.

11 Sélectionnez **Paramètres de l'application On-premises MDM > Exposer une API**.

12 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**. **Enregistrez** les paramètres.

13 Vous pouvez sélectionner et attribuer des licences Premium dans Azure.

a Dans la console Microsoft Azure, sélectionnez **Azure Active Directory > Licences** et sélectionnez **Tous les produits**. Sélectionnez la licence adéquate dans la liste.

b Sélectionnez **Attribuer**, sélectionnez les utilisateurs ou les groupes pour la licence, puis cliquez sur **Attribuer**.

14 Copiez l'**ID de répertoire** et le domaine principal pour accéder à Workspace ONE UEM Console.

a Accédez à l'onglet **Propriétés**, recherchez l'**ID de répertoire** Azure et copiez-le.

b Sélectionnez **Noms de domaine personnalisés** et copiez le **nom** signalé en tant que domaine principal.

15 Retournez à Workspace ONE UEM Console et sélectionnez **Utiliser Azure AD pour les services d'identité** pour configurer l'intégration d'Azure AD.

16 Entrez l'ID de répertoire que vous avez copié dans la zone de texte **ID du répertoire**.

17 Entrez le domaine principal que vous avez copié dans la zone de texte **Nom du locataire**.

18 Pour terminer la procédure, sélectionnez **Enregistrer**.

Enrôlement d'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. Pour plus d'informations sur l'enrôlement d'un terminal géré dans Azure AD, consultez la section Enrôler un terminal Azure AD géré dans Workspace ONE UEM.

Procédure

1. Sur le terminal Windows 10, 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 préalables

- Windows 10 – 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**.

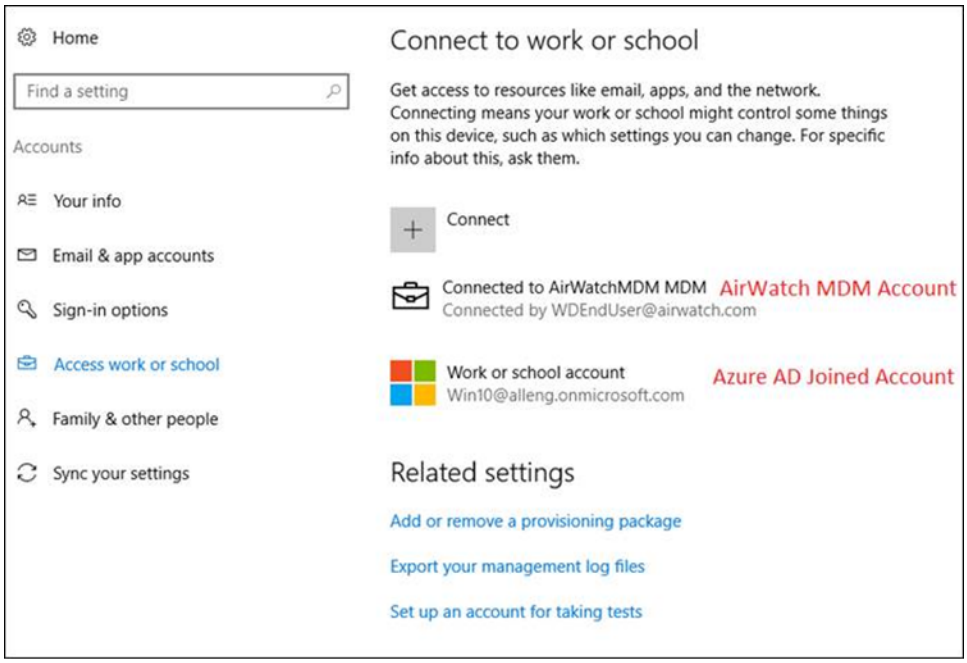
   Vous pouvez également vous enrôler par le biais de Workspace ONE Intelligent Hub pour Windows.

2 Terminez le processus d'enrôlement. Vous devez saisir une adresse e-mail avec un domaine différent de celui de votre compte Azure AD.

   a Si vous utilisez Windows Auto Discovery, consultez la section Enrôlement par l'intermédiaire de Work Access avec Windows Auto Discovery.

   b Si vous n'utilisez pas Windows Auto-Discovery, consultez la section Enrôlement par l'intermédiaire de Work Access avec Windows Auto Discovery.

3 Naviguez vers **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)

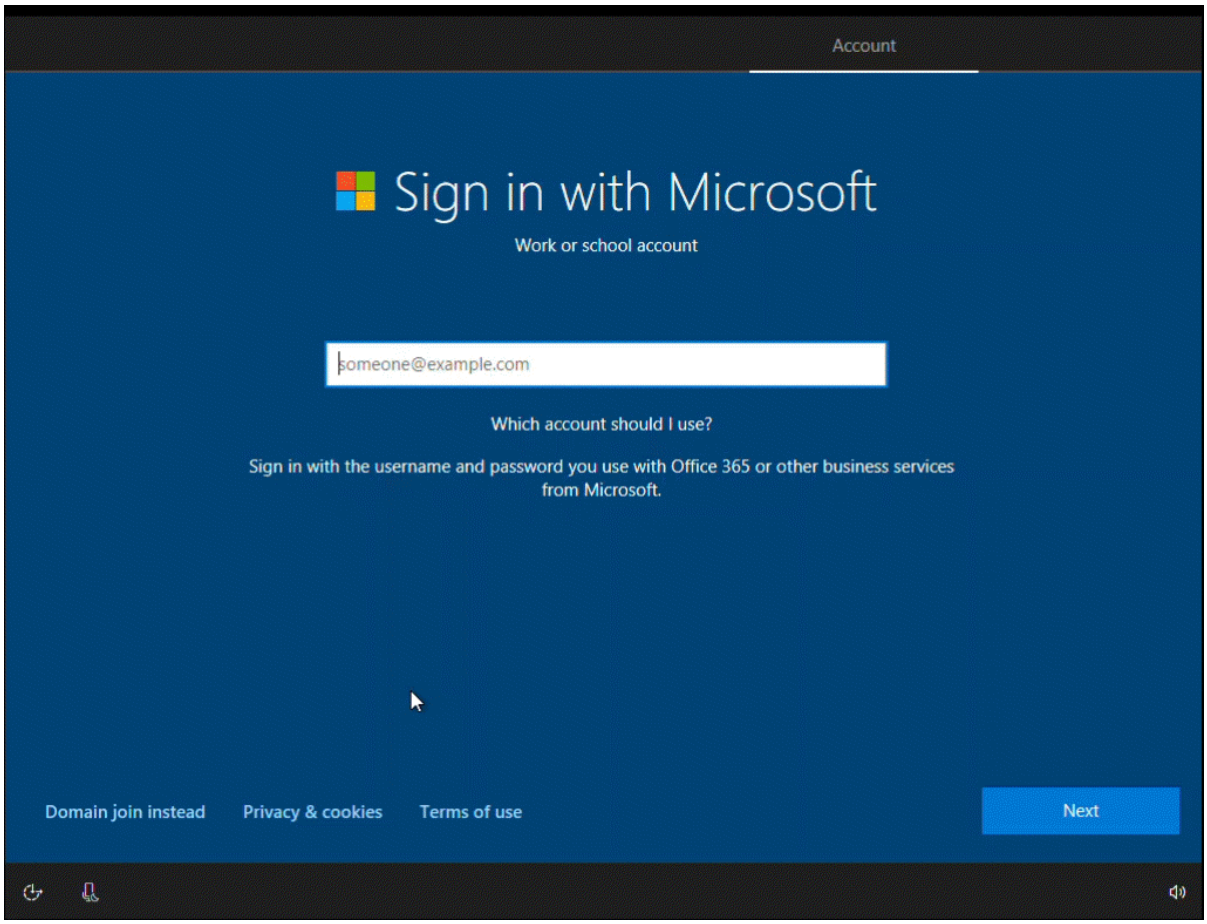
L'enrôlement en mode OOBE (Out-of-Box Experience) permet d'enrôler automatiquement un terminal dans le groupe organisationnel approprié au cours de la configuration initiale d'un terminal Windows 10.

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 ou vous serez déconnecté de force du terminal et obligé de réinitialiser celui-ci.

Conditions préalables

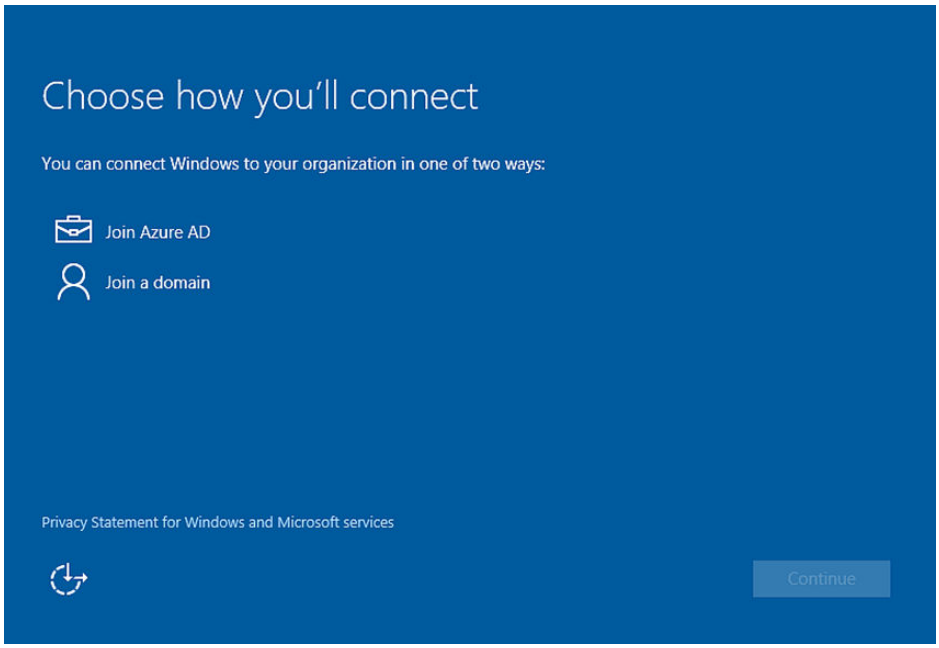
Le processus OOBE peut prendre un certain temps sur les terminaux des utilisateurs finaux. Envisagez d'activer l'affichage de la progression pour le statut de l'installation. Cet affichage permet aux utilisateurs finaux de savoir où ils en sont dans le processus. Pour activer l'affichage, accédez à **Groupes 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**.



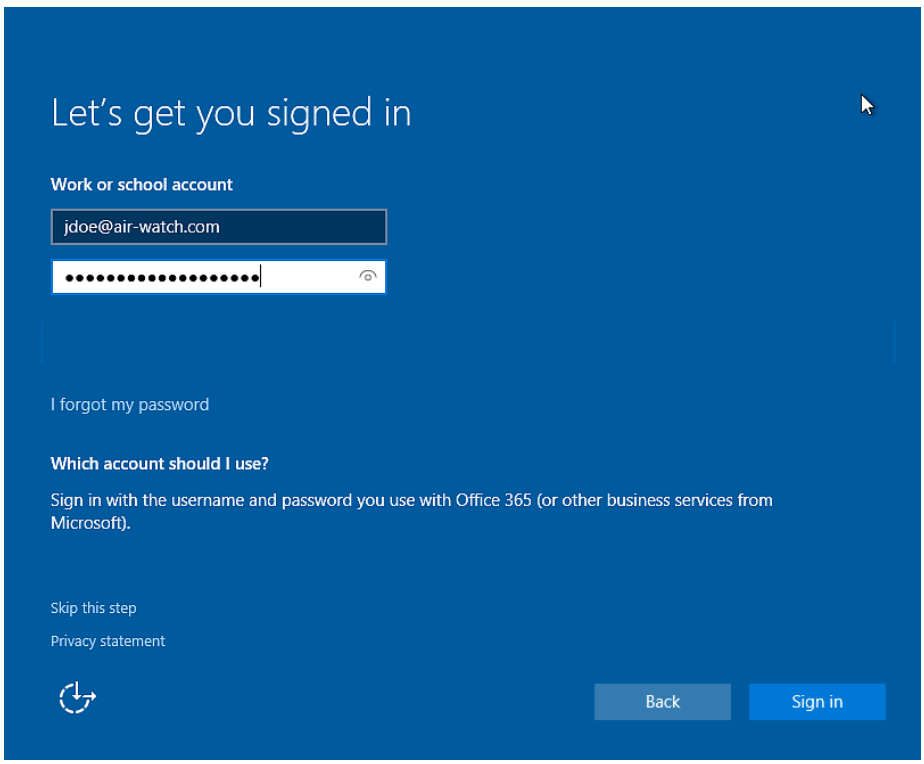
Procédure

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



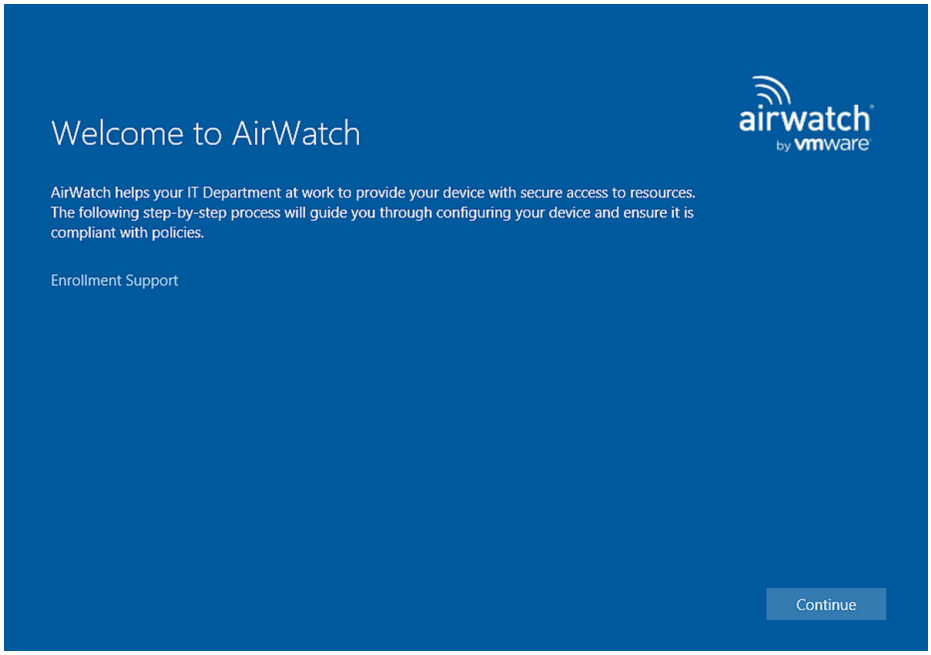
2 Sélectionnez **Joindre Azure AD**. Sélectionnez **Continuer**.

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 **J'accepte** si les termes du contrat sont activés.

7 Sélectionnez **Joindre** pour confirmer l'enrôlement à Workspace ONE UEM.

8 Sélectionnez **Terminer** pour finaliser l'enrôlement de votre terminal à Workspace ONE UEM. Votre terminal télécharge à présent les politiques et profils applicables.

Étape suivante

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 de bienvenue de Workspace ONE UEM apparaît. 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 dans Workspace ONE UEM. Votre terminal télécharge à présent les politiques et profils applicables.

Déploiement et enrôlement par lots

Le provisionnement par lots permet de créer un package préconfiguré qui préenrôle les terminaux Windows 10, puis les enrôle dans Workspace ONE UEM. Utilisez le provisionnement par lots pour enrôler et configurer rapidement 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 10 dans Workspace ONE UEM. Une fois le module installé, le terminal s'enrôle automatiquement dans Workspace ONE UEM.

Procédure

1. Téléchargez le kit Microsoft Assessment and Deployment Kit pour Windows 10 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.

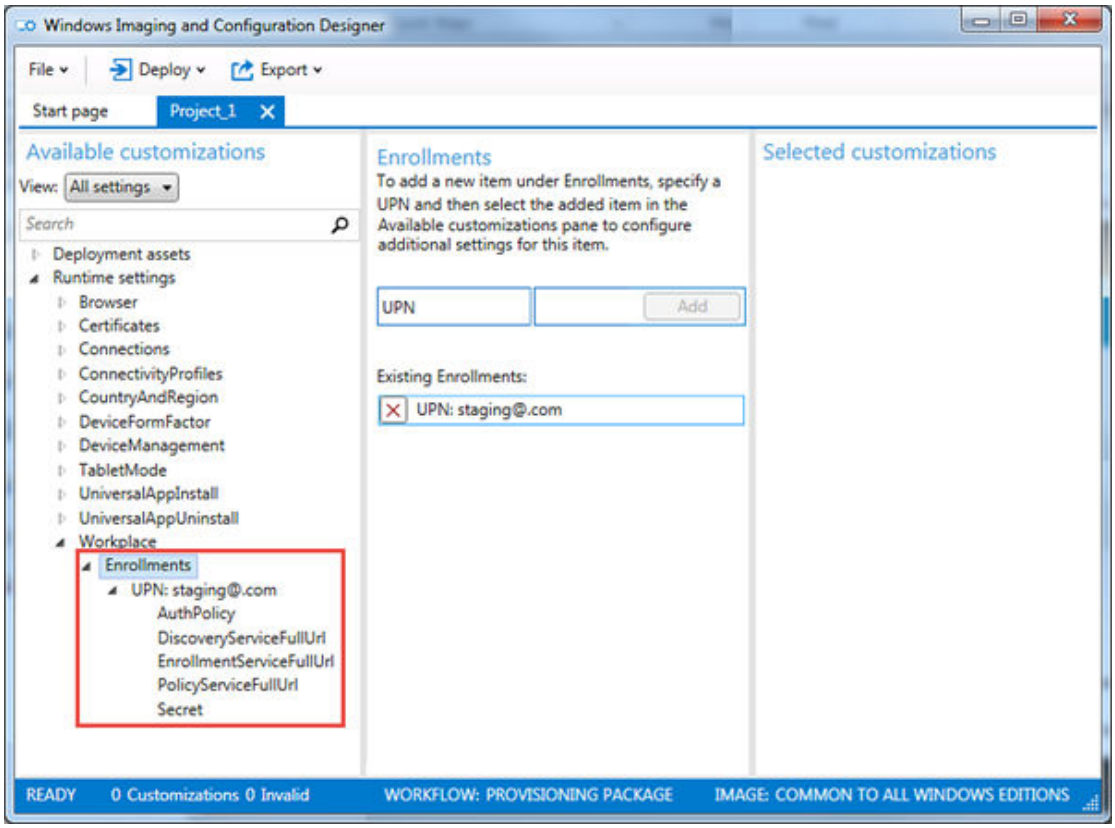
   Le choix type est l'option **Commun à toutes les éditions de Windows Desktop**.
4. (Facultatif) Importez un module de provisionnement pour créer un module de provisionnement basé sur les paramètres d'un module précédent.
5. Naviguez vers **Paramètres d'exécution > Espace de travail > Enrôlements**.

6 Dans Workspace ONE UEM Console, naviguez vers **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Windows > Windows Desktop > Préenrôlement et provisionnement**.

Lorsque vous naviguez vers cette page de paramètres, un utilisateur de préenrôlement est créé et les URL associées à l'utilisateur du préenrôlement créé apparaissent. 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 :

a Sélectionnez **AuthPolicy**, puis sélectionnez la valeur affichée dans UEM console.

b Sélectionnez **DiscoveryServiceFullURL**, puis copiez l'URL affichée dans UEM console.

c Sélectionnez **EnrollmentServiceFullURL**, puis copiez l'URL affichée dans UEM console.

d Sélectionnez **PolicyServiceFullURL**, puis copiez l'URL affichée dans UEM console.

e Sélectionnez **Secret**, puis copiez la valeur affichée dans 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.

Étape suivante

Installez ensuite le package de provisionnement par lots. Pour plus d'informations, consultez la section Installer des packages de provisionnement.

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.

Procédure

1 Sur le terminal à provisionner, naviguez vers **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 10 enrôlés via le Workspace ONE Intelligent Hub ou OOBE sont gérés par défaut par le 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 l'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 gestion MDM, notamment Workspace ONE Assist, VMware Workspace ONE Tunnel, la gestion de l'expérience des employés numériques et les services Workspace ONE Hub.

Procédure

1. Dans le Workspace ONE UEM Console, sélectionnez le groupe organisationnel à activer avec l'enrôlement en Mode Enregistré et accédez à **Terminaux > Paramètres des terminaux > 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.

États d'inscription Windows 10

La Workspace ONE UEM Console affiche un **État d'inscription** spécifique et un **État de jeton** spécifique sur la page **État d'inscription** pour représenter la progression de l'inscription d'un terminal Windows 10.

- Type d'enrôlement
- Type de terminal
- Cycle de vie de l'inscription
- La console affiche les états SET.

Type d'enrôlement

Si vous examinez les paramètres d'inscription dans les pages **Terminaux > Paramètres du terminal > Terminaux et utilisateurs > Général > Inscription**, vous voyez trois scénarios d'inscription généraux pour les terminaux Windows 10.

- **Inscription ouverte**

  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'inscription des terminaux correspond au processus d'ajout de terminaux professionnels dans Workspace ONE UEM Console avant leur inscription. 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 guide la manière dont le système Workspace ONE UEM suit et affiche l'état d'inscription du terminal.

- Terminaux sur liste blanche : l'administrateur de Workspace ONE UEM ajoute une liste de terminaux pré-approuvés pour s'inscrire.
- Terminaux sur liste noire : l'administrateur de Workspace ONE UEM ajoute une liste de terminaux qui ne sont pas autorisés à s'inscrire.
- 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 les 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'inscription

L'inscription des terminaux avec Workspace ONE UEM est composée de trois étapes générales.

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 inscrivent les terminaux avec Workspace ONE UEM.

3 Les utilisateurs ou les administrateurs désinscrivent les terminaux avec Workspace ONE UEM.

La console affiche les états SET.

Le type d'inscription, le type de terminal et l'étape d'inscription déterminent l'**État d'inscription** et l'**État du jeton** affichés pour les terminaux Windows 10 sur les pages **Terminaux > Cycle de vie > État d'inscription**.

- Tableau 2-3. 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 blanche	**Enregistré**	**Conforme**	**Inscrit**	**Conforme**	**Désinscrit**	**Conforme**
Terminal sur liste noire	**Sur liste noire**	**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.	**Enregistré**	**Enregistrement actif**	**Inscrit**	**Enregistrement actif**	**Enregistré**	**Enregistrement actif**
Terminal enregistré avec des attributs Les attributs sont le numéro de série, l'IMEI et l'UDID.	**Enregistré**	**Enregistrement actif**	**Inscrit**	**Enregistrement actif**	**Enregistré**	**Enregistrement actif**

- Tableau 2-4. 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 blanche	**Enregistré**	**Conforme**	**Inscrit**	**Conforme**	**Désinscrit**	**Conforme**
Terminal sur liste noire	**Sur liste noire**	**Non conforme**	**Non applicable**	**Non applicable**	**Non applicable**	**Non applicable**

Tableau 2-4. Terminaux enregistrés uniquement (pas de jeton) (suite)

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.	**Enregistré**	**Enregistrement actif**	**Inscrit**	**Enregistrement actif**	**Enregistré**	**Enregistrement actif**
Terminal enregistré avec des attributs Les attributs sont le numéro de série, l'IMEI et l'UDID.	**Enregistré**	**Enregistrement actif**	**Inscrit**	**Expiré**	**Enregistré**	**Enregistrement actif**

- Tableau 2-5. 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.	**Enregistré**	**Enregistrement actif**	**Inscrit**	**Non applicable**	**Désinscrit**	**Enregistrement expiré**
Terminal enregistré avec des attributs Les attributs sont le numéro de série, l'IMEI et l'UDID.	**Enregistré**	**Enregistrement actif**	**Inscrit**	**Non applicable**	**Désinscrit**	**Enregistrement expiré**

Profils Workspace ONE UEM pour Windows

3

Les profils sont le principal moyen de configurer vos terminaux Windows 10 pour la connexion au Wi-Fi, l'utilisation d'un VPN, la restriction de l'accès aux paramètres, etc. Apprenez à configurer les profils pour que vos terminaux Windows Desktop restent sécurisés.

Aperçu

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

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

Les profils 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 peuvent uniquement s'appliquer au niveau utilisateur ou au niveau terminal. 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.

Ce chapitre contient les rubriques suivantes :

- Configurer un profil Mode d'application unique (Windows Desktop)
- Configurer un profil Antivirus (Windows Desktop)
- Profil Chiffrement (Windows Desktop)
- Configurer un profil Mises à jour Windows (Windows Desktop)
- Configurer un profil de proxy (Windows Desktop)
- Configurer un profil Raccourcis Internet (Windows Desktop)
- Profil Exchange ActiveSync (Windows Desktop)
- Profil SCEP (Windows Desktop)
- Profil Contrôle d'applications (Windows Desktop)
- Configurer un profil Services Web Exchange (Windows Desktop)
- Créer un profil Gestion des licences Windows (Windows Desktop)
- Configurer un profil BIOS (Windows Desktop)
- Configuration du profil Mises à jour OEM (Windows Desktop)
- Configurer un profil de kiosque (Windows Desktop)
- Configurer un profil de personnalisation (Windows Desktop)
- Peer Distribution avec Workspace ONE
- Utiliser les paramètres personnalisés (Windows Desktop)

Configurez un profil avec code secret pour les terminaux Windows 10

Utilisez un profil avec code secret pour protéger vos terminaux Windows 10 en exigeant un code secret à chaque fois qu'ils sortent d'un état inactif. Découvrez comment un profil avec code secret avec Workspace ONE UEM garantit que toutes vos informations d'entreprise sensibles sur les terminaux gérés restent protégées.

Les codes secrets définis uniquement à l'aide de ce profil prendront effet si le code secret est plus strict que ceux existants. Par exemple, si l'actuel code d'accès au compte Microsoft nécessite des paramètres plus stricts que les exigences de la section de configuration Code d'accès, le terminal continue à utiliser le code d'accès au compte Microsoft.

Important la section de configuration du code d'accès ne s'applique pas aux terminaux joints au domaine.

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 **Code d'accès**.

6 Configurez les paramètres de code d'accès :

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 code d'accès 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 code d'accès.
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 10	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.

Configurer un profil Wi-Fi pour les terminaux Windows 10

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.

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 **Wi-Fi**.

6 Configurez les paramètres dans l'onglet **Général** :

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.
Port	Saisissez le port du proxy.

Paramètres	Descriptions
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. Cela permet de limiter les attaques de type MITM.
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. Pour plus d'informations, consultez la section Profil Identifiants Workspace ONE UEM pour les terminaux Windows 10. 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.

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

Configurer un profil VPN pour les terminaux Windows 10

Workspace ONE UEM prend en charge la configuration des paramètres VPN de terminal afin que les utilisateurs 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.

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** ou **Profil du terminal**.
4. Configurez les **paramètres généraux** du profil.
5. Sélectionnez le profil **VPN**.
6. Configurez les paramètres **Informations de connexion** :

Paramètres	Descriptions
Nom de la connexion	Saisissez le nom de la connexion VPN.
Type de connexion	Sélectionnez le type de connexion VPN :
Serveur	Saisissez le nom d'hôte ou l'adresse IP du serveur VPN.
Port	Saisissez le port utilisé par le serveur VPN.
Paramètres de connexion avancés	Autorisez la configuration de règles avancées de routage pour les connexions VPN du terminal.
Adresses de routage	Sélectionnez **Ajouter** pour saisir 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 saisir 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** (Force Tunnel) : pour cette règle de trafic, tout le trafic IP doit passer par l'interface VPN uniquement. ■ **Autoriser l'accès direct aux ressources externes** (Split Tunnel) : pour cette règle de filtrage de trafic, seul le trafic réservé à l'interface VPN (déterminé par la pile réseau) passe par 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	Saisissez l'adresse IP du serveur de proxy. Apparaît lorsque le **proxy** est défini sur **Manuel**.
URL de configuration du serveur proxy	Saisissez l'URL pour les paramètres de configuration du serveur proxy. Apparaît lorsque le **proxy** est défini sur **Manuel**.
Contournement local du proxy	Activez le contournement du serveur proxy lorsque le terminal détecte qu'il est sur le réseau local.

Paramètres	Descriptions
Protocole	Sélectionnez le protocole d'authentification à utiliser avec le VPN : ■ EAP – Autorise différentes 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	Cliquez sur **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 de certificats dans laquelle l'utilisateur choisit. 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 ce du terminal Windows. Apparaît lorsque **Type EAP** est défini sur **EAP-MSCHAPv2**.
Confidentialité d'identité	Saisissez 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 du client 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. Pour en savoir plus sur le VPN par application, voir VPN par application pour les terminaux Windows 10 utilisant le profil VPN

Paramètres	Descriptions
ID d'application	Sélectionnez tout d'abord si l'application est une application de magasin 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 au fichier : %ProgramFiles%/ Internet Explorer/iexplore.exe ■ Nom de 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 vous connecter automatiquement à la connexion VPN dès le 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 d'application. 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** : liste de valeurs séparées par des virgules spécifiant la plage d'adresses IP distantes à autoriser. ■ **Ports** : liste de valeurs séparées par des virgules spécifiant la plage de ports distants 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 en savoir plus sur le fonctionnement de ces filtres et politiques, ainsi que la logique utilisée, consultez la section VPN par application pour les terminaux Windows 10 utilisant le profil VPN.
Règles du VPN au niveau des terminaux	Cliquez sur **Ajouter** pour ajouter des règles de trafic à tout le 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** : liste de valeurs séparées par des virgules spécifiant la plage d'adresses IP distantes à autoriser. ■ **Ports** : liste de valeurs séparées par des virgules spécifiant la plage de ports distants 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 de 0-255 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 mes identifiants	Activez ce paramètre pour mémoriser les identifiants de connexion.

Paramètres	Descriptions
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, jamais déconnecté, 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 local.
Détection de réseaux approuvés	Saisissez les adresses réseau approuvées, 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 (sur liste blanche) ou Edge (pas sur liste blanche). 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.

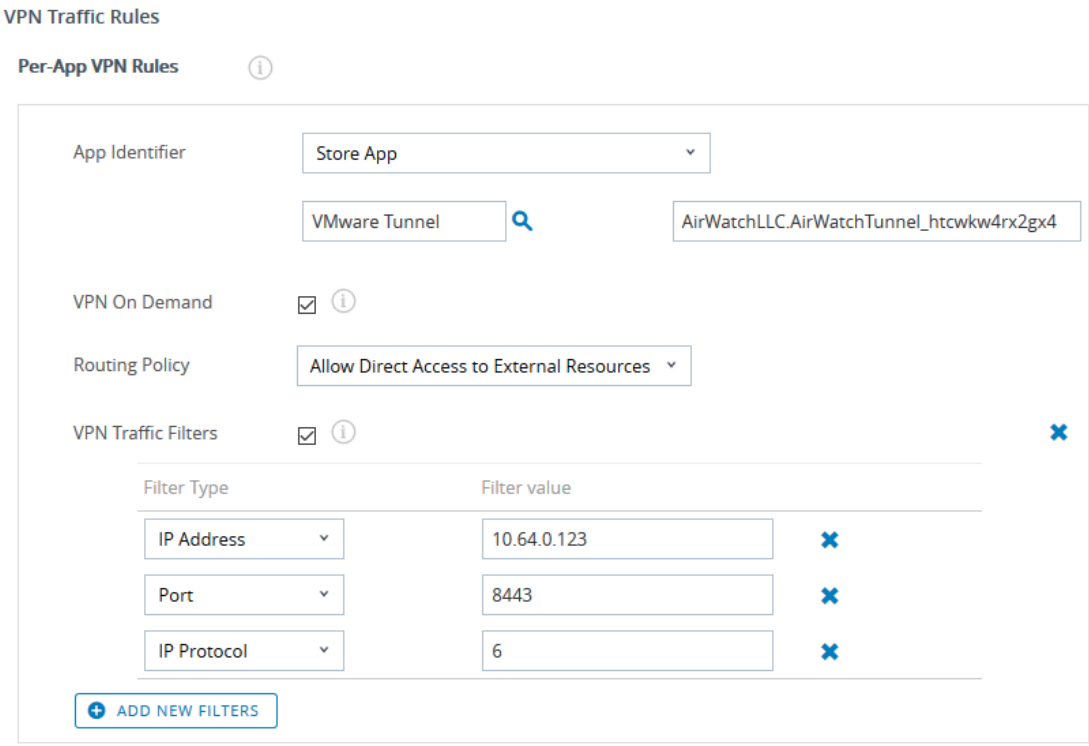
VPN par application pour les terminaux Windows 10 utilisant le profil VPN

Les profils VPN Workspace ONE UEM prennent en charge la configuration des paramètres VPN par application pour les terminaux Windows 10. 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

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 Identifiants Workspace ONE UEM pour les terminaux Windows 10

Un profil Identifiants vous permet de déployer des certificats racine, intermédiaire et client sur les terminaux Windows 10 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 10.

Même avec des codes d'accès 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.

Configurez un profil Identifiants pour les terminaux Windows 10

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 les magasins de certificat personnels, intermédiaires, de racines de confiance, de serveurs de publication approuvés et de personnes de confiance. Apprenez à configurer un profil Identifiants pour activer l'authentification pour vos terminaux Windows 10.

Même avec des codes d'accès 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.

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** 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 **Importer**, vous devez importer un nouveau certificat. ■ Si vous sélectionnez **Autorité de certification définie**, vous devez choisir une autorité de certification prédéfinie, ainsi qu'un modèle de certificat. ■ 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**.
Exporter la clé privée	Sélectionnez **Autoriser** pour permettre aux utilisateurs d'exporter des certificats à l'aide du Gestionnaire de certificats Windows. Sélectionnez **Interdire** pour empêcher les utilisateurs d'exporter des certificats.
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.

Paramètres	Descriptions
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 du secteur de configuration 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.
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.

Configurer une charge utile de restrictions pour les terminaux Windows 10

Utilisez les profils de restrictions pour désactiver l'accès des utilisateurs finaux aux fonctionnalités du terminal afin que vos terminaux Windows 10 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.

Procédure

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 se désenrôler manuellement de Workspace ONE UEM via l'enrôlement Espace de travail/accès professionnel. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
La configuration en cours du Hub installe les packages de provisionnement.	Activez ce paramètre pour autoriser l'utilisation de packages de provisionnement dans le cadre de l'enrôlement de terminaux dans Workspace ONE UEM (provisionnement par lots). Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Emplacement	Sélectionnez le fonctionnement des services de localisation sur le terminal. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Envoyer les données de télémétrie concernant le diagnostic et l'utilisation	Sélectionnez le niveau des données de télémétrie à envoyer à Microsoft. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Date/heure	Autorisez l'utilisateur à changer les paramètres Date/heure. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Langue	Autorisez l'utilisateur à changer les paramètres de langue. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.

Paramètres	Description
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Région	Autorisez l'utilisateur à modifier la région. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Autorisez l'utilisateur à modifier les options de connexion.	Autorisez l'utilisateur à modifier les options de connexion. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
VPN	Autorisez l'utilisateur à changer les paramètres de VPN. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Autoriser l'utilisateur à modifier les paramètres de compte	Autorisez l'utilisateur à modifier les paramètres de compte. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Bluetooth	Autorisez l'utilisation du Bluetooth sur le terminal. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Publicité Bluetooth de terminal	Autorisez le terminal à diffuser les annonces Bluetooth. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Les terminaux compatibles avec Bluetooth peuvent découvrir le terminal	Autorisez la détection du Bluetooth par d'autres terminaux Bluetooth. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
appareil photo	Autorisez l'accès à la fonction appareil-photo du terminal. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Cortana	Autorisez l'accès à l'application Cortana. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.

Paramètres	Description
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 codes d'accès. **Note** 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. La restriction ne s'applique pas aux terminaux Windows 10 Famille.
Rechercher pour utiliser les informations de localisation.	Autorisez la recherche à utiliser les informations d'emplacement de terminal. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Carte de stockage	Activez ce paramètre pour autoriser l'utilisation d'une carte SD et des ports USB de l'appareil. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Paramètres de synchronisation Windows	Autorisez l'utilisateur à synchroniser les paramètres Windows entre terminaux. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Conseils Windows	Autorisez les conseils Windows sur le terminal pour assister l'utilisateur. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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. Cette restriction s'applique à tous les terminaux Windows 10.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.

Paramètres	Description
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Autoriser la diffusion DVR de jeux vidéo	Activez ce paramètre pour autoriser l'enregistrement et la diffusion de jeux sur le terminal. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Données mobiles en itinérance	Activez ce paramètre pour autoriser l'utilisation de données mobiles en itinérance. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Partage Internet	Activez ce paramètre pour autoriser le partage Internet entre terminaux. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Itinérance VPN sur le réseau mobile	Autorisez l'utilisation d'un VPN lors de connexions de données cellulaires en itinérance. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.

Paramètres	Description
Saisie automatique	Autorisez l'utilisation de remplissage automatique des informations utilisateur. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Cookies	Autorisez l'utilisation de cookies. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Ne pas suivre	Autorisez l'utilisation de demandes DNT. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Gestionnaire de mots de passe	Autorisez l'utilisation du gestionnaire de mots de passe. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Pop-ups	Autorisez les fenêtres locales de navigateur. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
Suggestions de recherche dans la barre d'adresses	Autorisez l'affichage des suggestions de recherche dans la barre d'adresse. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
SmartScreen	Autorisez l'utilisation du filtre de contenu et d'emplacements malveillants SmartScreen. Cette restriction s'applique uniquement aux terminaux Windows 10 et n'est pas prise en charge pour les terminaux Windows 10 Famille.
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 Windows Defender Exploit Guard pour les terminaux Windows 10

Protégez vos terminaux Windows 10 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 10 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 10. 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.

Créer un profil Defender Exploit Guard pour les terminaux Windows 10

Créez un profil Defender Exploit Guard avec Workspace ONE UEM pour protéger vos terminaux Windows 10 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 10.

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 préalables

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 **?**

a Ajoutez des dossiers supplémentaires à protéger en sélectionnant **Ajouter** et saisissez le chemin d'accès au fichier de dossiers.

b 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.

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.

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 de protection des données Workspace ONE UEM pour les terminaux Windows 10

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 10.

La protection des données place les applications d'entreprise sur liste blanche, 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 figurant dans la liste blanche 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'ajouter au cas par cas les applications autorisées dans la liste blanche 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 ajoutez des applications exemptées à la liste blanche. Les applications exemptées créent des écarts dans la protection de données et la fuite des données d'entreprise.

- Applications non autorisées – Ces applications ne figurent pas dans la liste blanche, 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.

Configurer un profil Protection des données (Windows Desktop)

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.

Procédure

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 section de configuration **Protection des données d'entreprise**.
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 ajoute en liste blanche toutes les applications de cet éditeur.
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 packages (PFN) de l'application.

Paramètres	Descriptions
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 10 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. Pour plus d'informations, voir Créer un certificat de système de fichiers EFS (Windows Desktop).

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

Créer un certificat de système de fichiers EFS (Windows Desktop)

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.

Procédure

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>`

La valeur <EFSRA> est 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. Pour plus d'informations, voir Configurer un profil Protection des données (Windows Desktop).

Profil Windows Hello (Windows Desktop)

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 10 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 10 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.

Créer un profil Windows Hello (Windows Desktop)

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.

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 **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 for Work 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.

Configurer un profil Pare-feu (Hérité) (Windows Desktop)

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.

Conditions préalables

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

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 **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.
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.

Configurer un profil Pare-feu (Windows Desktop)

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 place automatiquement sur liste blanche l'agent OMA-DM pour assurer que le Workspace ONE UEM Console peut toujours communiquer avec les terminaux.

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 **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.
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.

Paramètre	Description
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.
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.

Configurer un profil Mode d'application unique (Windows Desktop)

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.

Conditions préalables

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 **Mode d'application unique** :

Paramètres	Descriptions
Nom d'application	Saisissez le nom convivial de l'application. Pour les applications Windows, le nom convivial est le Nom du package ou l'ID du package. 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 la forme « nom ».

7 Après avoir configuré un profil Mode d'application unique, vous devez configurer un mode d'application unique sur le terminal.

   a Une fois le profil Mode d'application unique reçu sur le terminal, redémarrez ce dernier pour commencer.

   b 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.

Configurer un profil Antivirus (Windows Desktop)

La création d'un profil d'**antivirus** permet de configurer 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 Antivirus Windows Defender natif, pas les autres programmes antivirus tiers.

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 **Antivirus**.

6 Configurez les paramètres dans l'onglet **Antivirus** :

Paramètres	Descriptions
Surveillance en temps réel	Activez ce paramètre pour que Antivirus Windows Defender surveille le terminal en temps réel.
Sens d'analyse en temps réel	Activez ce paramètre pour que 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.

Paramètres	Descriptions
Niveau de protection du cloud	Activez ce paramètre pour configurer le degré d'agressivité de 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 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 d'accès ou processus à exclure des analyses Antivirus Windows Defender. Sélectionnez **Ajouter nouveau** pour ajouter une exception.

Paramètres	Descriptions
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 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. 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 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 Antivirus Windows Defender surveille les applications potentiellement indésirables (PUA) sur les clients finaux. ■ **Protection IOAV** : activez ce paramètre pour protéger Antivirus Windows Defender contre la manipulation.

Paramètres	Descriptions
	Cet élément de menu détecte et empêche les modifications des paramètres de sécurité sur les clients finaux. Il est également appelé protection contre la manipulation. ■ **Protection OnAccess** : activez ce paramètre pour que Antivirus Windows Defender protège les fichiers et les dossiers contre tout accès non autorisé. ■ **Protection du Cloud** : activez ce paramètre pour que 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 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 Antivirus Windows Defender analyse des lecteurs réseau mappés vers des terminaux. ■ **Analyser les archives** : activez ce paramètre pour que Antivirus Windows Defender exécute une analyse complète sur des dossiers archivés. ■ **Analyser les lecteurs amovibles** : activez ce paramètre pour que 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 Chiffrement (Windows Desktop)

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

Le chiffrement BitLocker est uniquement disponible sur les terminaux Windows 8 Entreprise et Professionnel, ainsi que sur Windows 10 Entreprise, Éducation et Professionnel.

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 le 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 détecte que le terminal n'est pas chiffré, il le chiffre automatiquement.

Si vous choisissez de chiffrer à l'aide de BitLocker, une clé de récupération créée lors du chiffrement est stockée dans Workspace ONE UEM Console et dans le portail self-service.

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

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

Attention Windows 10 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 fait appel au Module de plateforme sécurisée (TPM) pour stocker le mot de passe de récupération sur le terminal afin de déchiffrer les disques durs connectés à la carte mère. Si le lecteur est retiré de la carte mère, il ne sera pas déchiffré. Pour une authentification améliorée, vous pouvez activer un code PIN de chiffrement afin de confirmer l'authentification de l'utilisateur. Vous pouvez également exiger un mot de passe pour les terminaux comme solution de secours au cas où TPM serait indisponible.

Comportement du déploiement

Le chiffrement BitLocker natif Windows permet de sécuriser les données sur les terminaux Windows Desktop. Le déploiement du profil Chiffrement nécessite des actions supplémentaires de la part de l'utilisateur.

Si le profil chiffrement est envoyé à un terminal chiffré et que les paramètres de chiffrement actuels correspondent à ceux du profil, Workspace ONE Intelligent Hub ajoute une nouvelle clé de récupération et l'envoie à Workspace ONE UEM Console. Cette nouvelle clé est également stockée dans une base de données chiffrée sur le terminal. Grâce à cette fonctionnalité, si un utilisateur ou un administrateur essaie de déchiffrer le terminal, le profil Chiffrement le rechiffre à l'aide de la nouvelle clé. 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 nouvelle version du profil Chiffrement à un terminal géré par un profil Chiffrement existant. La méthode de chiffrement existante est conservée.

État du chiffrement

Si BitLocker est activé et en cours d'utilisation, vous pouvez visualiser des rapports sur le statut de chiffrement dans les zones suivantes :

- Tableau de bord Workspace ONE UEM
  - Les détails du terminal affichent des informations sur la clé de récupération.
  - La protection BitLocker apparaît comme activée.
- Workspace ONE UEMPortail self-service
  - Le portail self-service indique que la clé de récupération est stockée, mais pas les détails concernant la clé.
  - La protection BitLocker apparaît comme activée.

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. L'effacement 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 choisir d'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.

Configurer un profil Chiffrement (Windows Desktop)

Créez un profil Chiffrement pour sécuriser vos données sur les terminaux Windows Desktop à l'aide du chiffrement BitLocker natif.

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 **Chiffrement** et configurez les paramètres :

Paramètres	Descriptions
Volume chiffré	Utilisez le menu déroulant pour sélectionner le type de chiffrement comme suit : ■ Tous les disques durs fixes – Chiffre la totalité du disque dur sur le terminal, y compris la partition système sur laquelle est installé le système. ■ Partition système – Chiffre une partition ou un disque, dans l'emplacement d'installation et de démarrage de Windows.
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.
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.
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 déverrouiller le terminal. Cette option bloque 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	Descriptions
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 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 déchiffrer 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 statique : Créer une clé BitLocker statique	Sélectionnez cette case à cocher 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 ce que la clé de récupération change.
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.
Interruption de BitLocker : Activer l'interruption de BitLocker	Sélectionnez cette case à cocher pour activer l'interruption 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.
Interruption de BitLocker : Interrompre le type BitLocker	Sélectionnez le type d'interruption. ■ **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.
Interruption de BitLocker : Heure de début d'interruption de BitLocker	Saisissez la date/heure de début de l'interruption de BitLocker.

Paramètres	Descriptions
Interruption de BitLocker : Heure de fin d'interruption de BitLocker	Saisissez la date/heure de fin de l'interruption de BitLocker.
Interruption de BitLocker : Type de répétition planifiée	Définissez si l'interruption planifiée doit être répétée de manière quotidienne ou hebdomadaire. Si vous choisissez une répétition hebdomadaire, sélectionnez les jours de la semaine impliqués.

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

Configurer un profil Mises à jour Windows (Windows Desktop)

Créez un profil Mises à jour Windows vous permet de configurer les paramètres des mises à jour Windows sur les terminaux Windows Desktop. Le profil garantit que tous les terminaux sont à jour, ce qui améliore la sécurité des terminaux et du serveur.

Pour configurer les paramètres avancés de Mises à jour Windows, utilisez le gestionnaire de terminaux Windows.

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 10 : https://technet.microsoft.com/en-us/windows/release-info.aspx.

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 **Mises à jour Windows**.

6 Configurez les paramètres Mises à jour Windows :

Paramètres	Descriptions
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 saisissez 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 - Lente ■ Branche Windows Insider - Rapide ■ Lancement du build Windows Insider
Builds Insider	Autorisez le téléchargement de builds Windows Insider 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 10 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 transférez le profil vers un terminal exécutant une version de Windows 10 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 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.
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.

Paramètres	Descriptions
Activer les paramètres pour les versions précédentes de Windows	Sélectionnez cette option pour activer les paramètres d'échelonnement pour des versions précédentes de Windows. Les paramètres incluent les éléments suivants : ■ **Différer les nouvelles fonctionnalités (par mois)** ■ **Différer les mises à jour (par semaine)** ■ **Mettre les échelonnements en pause**
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 ■ 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.
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**.
Échéances de redémarrage automatique	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.
Notifications de redémarrage automatique (minutes)	Définissez le nombre de minutes durant lesquelles un avertissement s'affiche avant un redémarrage automatique.
Notification de redémarrage automatique requis	Définissez comment une notification de redémarrage automatique doit être ignorée. ■ Rejet automatique : ignoré automatiquement. ■ Rejet de l'utilisateur : exige de l'utilisateur qu'il ferme la notification.
Délai du redémarrage amorcé	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.
Planification des répétitions de redémarrage amorcé	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)	Définissez le nombre d'heures durant lesquelles un avertissement aux utilisateurs s'affiche avant un redémarrage planifié.

Paramètres	Descriptions
Avertissement de redémarrage planifié (minutes)	Définissez le nombre de minutes durant lesquelles un avertissement aux utilisateurs s'affiche avant un redémarrage planifié.
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.
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.
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**. Pour plus d'informations, consultez la section Approuver les mises à jour Windows.

Paramètres	Descriptions
Mises à jour approuvées automatiquement	Activez cette option pour définir des groupes de mises à jour approuvés automatiquement pour le téléchargement sur les terminaux des utilisateurs finaux. 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. Lorsque vous activez cette option, les groupes de mise à jour s'affichent afin que vous puissiez définir ceux à mettre à jour automatiquement. Définissez ces groupes sur Autorisé pour approuver automatiquement les mises à jour à télécharger sur les terminaux attribués. ■ Mises à jour de fonctionnalités ■ Win32 ■ Connecteurs ■ Critique ■ Définition ■ Kit développeur ■ Pilotes ■ Feature Pack ■ Guide ■ Sécurité ■ Service Pack ■ Mises à jour des outils ■ Correctifs cumulatifs ■ Généralités
Mises à jour pair à pair	Autorise le téléchargement pair à pair de mises à jour.
Méthode Pair à pair autorisée	Sélectionnez la méthode de connexion pair à pair que vous souhaitez autoriser.
Limiter l'utilisation aux membres disposant du même ID de groupe	Limite le téléchargement pair à pair vers des terminaux du même groupe organisationnel.
Mise en cache des pairs via VPN	Activez cette option pour permettre aux terminaux de participer à la mise en cache des pairs lorsqu'ils sont connectés à un VPN.
Batterie minimale requise pour les téléchargements de pairs (%)	Sélectionnez le pourcentage minimal de charge de la batterie qu'un terminal doit avoir avant de pouvoir participer au chargement pair à pair.
Taille de cache maximale autorisée	Entrez la taille de cache maximale que l'optimisation de la livraison peut utiliser. Cette valeur représente un pourcentage de la taille du disque.
Taille maximale du cache que l'optimisation de la distribution peut utiliser (%)	Saisissez le pourcentage de cache que peut utiliser l'optimisation de la distribution.
Durée maximale de maintien des fichiers dans le cache d'optimisation de distribution (en secondes)	Définissez le nombre de secondes qu'un fichier est retenu dans le cache d'optimisation de la distribution avant d'être envoyé sur les terminaux. Le cache d'optimisation garde des mises à jour disponibles sur d'autres pairs auxquels le terminal à accès pour accélérer le téléchargement de mises à jour.

Paramètres	Descriptions
Mémoire minimale du disque du terminal pour utiliser la mise en cache des pairs	Entrez la taille de disque minimale (en Go) dont le terminal doit disposer pour utiliser la mise en cache des pairs.
Mémoire minimale de la RAM du terminal pour utiliser la mise en cache des pairs	Entrez la taille de RAM minimale (en Go) dont le terminal doit disposer pour utiliser la mise en cache des pairs.
Taille minimum du fichier de contenu que la mise en cache des pairs peut utiliser	Entrez la taille minimale du fichier de contenu pour que la mise en cache des pairs soit utilisée.
Emplacement du lecteur utilisé pour la mise en cache des pairs	Entrez l'emplacement du fichier à utiliser pour la mise en cache des pairs.
Bande passante d'importation maximale qu'un terminal utilisera pour toute activité de téléchargement concurrente (Ko/seconde)	Saisissez la bande passante d'importation maximale en Ko/seconde qu'utilise un terminal lors de l'envoi de mises à jour à des pairs.
Bande passante de téléchargement maximale qu'un terminal utilise (Ko/seconde)	Entrez la bande passante de téléchargement maximale en Ko/seconde qu'utilise un terminal lors du téléchargement de mises à jour des pairs.
Bande passante de téléchargement maximale en pourcentage du total disponible (%)	Entrez le pourcentage maximal de bande passante de téléchargement (de la bande passante totale disponible) utilisé pour le téléchargement des mises à jour par mise en cache des pairs.
QoS minimale pour les téléchargements en arrière-plan (Ko/seconde)	Entrez la qualité de service minimale (ou la vitesse) en Ko/seconde des téléchargements en arrière-plan.
Collecte mensuelle des données de téléchargement (Go)	Entrez la quantité maximale de données (en Go) qu'un terminal peut télécharger par mois.

7 Cliquez sur **Enregistrer et publier** pour envoyer le profil vers les 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 10. La page **Mises à jour du terminal** répertorie toutes les mises à jour disponibles pour les terminaux Windows 10 enrôlés dans le groupe organisationnel sélectionné.

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**.

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 10 enrôlés dans le groupe organisationnel sélectionné sont affichées. Si vous n'avez pas de terminal Windows 10 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.

Pour plus d'informations sur la révision et l'approbation des mises à jour Windows pour l'installation sur vos terminaux Windows 10, reportez-vous à Approuver les mises à jour Windows. 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**.

Tableau 3-1. Description de l'état des mises à jour de terminal Windows

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.

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.

Pour plus d'informations sur le déploiement des mises à jour OEM sur des terminaux, consultez Configuration du profil Mises à jour OEM (Windows Desktop)

Approuver les mises à jour Windows

Passez en revue et approuvez les mises à jour Windows pour les installer sur vos terminaux Windows 10. Cette fonction vous permet de garantir que vos terminaux restent à jour tout en contrôlant la distribution des mises à jour afin de répondre aux besoins de votre entreprise.

Pour plus d'informations sur les éléments affichés sur la page **Mises à jour du terminal**, reportez-vous à Mises à jour des terminaux pour Windows Desktop.

Conditions préalables

Vous devez publier un profil Mises à jour Windows avec l'option **Demander l'approbation de la mise à jour** activée.

Procédure

1. Accédez à **Ressources > Mises à jour du terminal > Windows**.
2. Sélectionnez la case à cocher sur la gauche de la mise à jour.

   Cocher la case affiche l'élément de menu **Attribuer**. Vous ne pouvez pas accéder à la fonctionnalité d'attribution si vous ne cochez pas cette case.
3. Cliquez sur le bouton **Attribuer**.
4. Saisissez les Smart Groups auxquels la règle s'applique.
5. Sélectionnez **Ajouter**.

Configurer un profil de proxy (Windows Desktop)

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

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 **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.

Paramètres	Description
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**.

Configurer un profil Raccourcis Internet (Windows Desktop)

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.

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 **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 Exchange ActiveSync (Windows Desktop)

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. Pour plus d'informations, reportez-vous à la section Configurez un profil Identifiants pour les terminaux Windows 10.

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 profil 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.

Configurer un profil Exchange ActiveSync (Windows Desktop)

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.

Note 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.

Procédure

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. Pour plus d'informations, reportez-vous à la section Nom d'utilisateur et mot de passe en bas de la page.
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. Pour plus d'informations, voir la section Configurer une charge utile d'informations d'identification.
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.
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 la console Workspace ONE UEM ou **Enregistrer et publier** pour transférer le profil sur les terminaux.

Profil SCEP (Windows Desktop)

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 codes d'accès 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.

Configurer un profil SCEP (Windows Desktop)

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

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** 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.

Paramètres	Descriptions
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 Contrôle d'applications (Windows Desktop)

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 mettre sur liste blanche ou sur liste noire des applications spécifiques. Alors que le moteur de conformité surveille les terminaux et y recherche les applications mises en liste blanche et en liste noire, le contrôle des applications empêche même 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 figurant dans la liste blanche. Les applications figurant sur la liste noire 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.

Configurer un profil Contrôle d'applications (Windows Desktop)

Activez le contrôle des applications pour mettre sur liste blanche ou sur liste noire 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 10.

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.

Conditions préalables

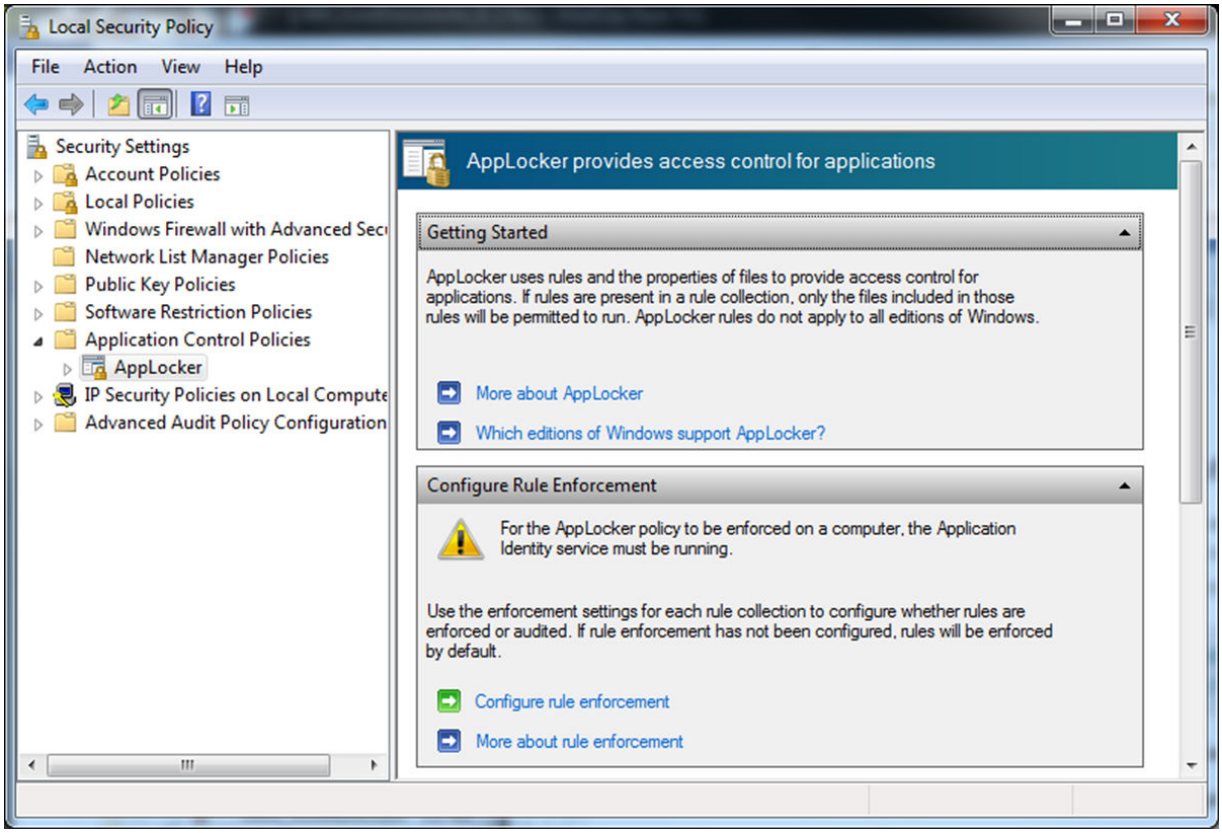
Pour configurer un fichier de configuration XML, vous devez configurer les paramètres Applocker sur un terminal et exporter le fichier à utiliser avec le profil.

Le profil Contrôle des applications requiert Windows 10 Entreprise ou Éducation.

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**.

Configurer un profil Services Web Exchange (Windows Desktop)

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.

Conditions préalables

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

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 **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.

Créer un profil Gestion des licences Windows (Windows Desktop)

Configurez un profil Gestion des licences Windows pour fournir aux terminaux Windows 10 une clé de licence Windows 10 Entreprise ou Windows 10 Éducation. Utilisez ce profil pour mettre à niveau les terminaux qui ne disposent pas de Windows 10 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 10 ne peut effectuer la mise à niveau que dans les configurations suivantes :

- Windows 10 Entreprise à Windows 10 Éducation
- Windows 10 Famille à Windows 10 Éducation
- Windows 10 Professionnel à Windows 10 Éducation
- Windows 10 Professionnel à Windows 10 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.

Configurer un profil BIOS (Windows Desktop)

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. Workspace ONE UEM transfère uniquement les paramètres pris en charge par un terminal. Si vous transférez ce profil vers des terminaux, Workspace ONE UEM transfère automatiquement l'application Dell Command | Monitor sur les terminaux.

Pour plus d'informations sur les terminaux pris en charge, reportez-vous à la section Chapitre 10 Intégration de Dell Command | Monitor.

Conditions préalables

Si vous souhaitez utiliser la fonctionnalité de module de configuration, vous devez déployer l'application Dell Command | Configure sur les terminaux. Pour plus d'informations, reportez-vous à Chapitre 9 Intégration de Dell Command | Configure.

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 **BIOS** et configurez les paramètres suivants :

Paramètres	Descriptions
Définition du mot de passe du BIOS	Sélectionnez **Géré** pour que Workspace ONE UEM génère automatiquement un mot de passe du BIOS fort et unique 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	Saisissez 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 TPM	Cliquez sur **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.
Mode de démarrage	Sélectionnez si le terminal doit démarrer en mode **BIOS** ou **UEFI**.
Protection du mode de démarrage	Sélectionnez **Activer** pour éviter les problèmes qui empêchent le démarrage de l'OS installé sur le terminal. Cette protection empêche de modifier le mode de démarrage d'un terminal sur lequel un OS est installé.
Démarrage sécurisé	Sélectionnez **Activer** pour utiliser les paramètres de démarrage sécurisé sur le terminal. Vous ne pouvez pas désactiver le démarrage sécurisé avec DCM. Si vos terminaux utilisent déjà le démarrage sécurisé, vous devez désactiver manuellement les paramètres du terminal. Pour utiliser le démarrage sécurisé, vous devez définir le **Mode de démarrage** sur **UEFI** et l'**Option ROMS héritée** sur **Désactiver**.
Option ROMS héritée	Sélectionnez **Activer** pour autoriser l'utilisation de l'option ROMS héritée lors du processus de démarrage.
Virtualisation CPU	Cliquez sur **Activer** pour autoriser la prise en charge de la virtualisation matérielle.
Virtualisation IO	Cliquez sur **Activer** pour autoriser la virtualisation en entrée/sortie.

Paramètres	Descriptions
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**.
LAN 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 la surveillance SMART des solutions de stockage du terminal.
Charge de batterie principale	Sélectionnez les règles de charge du terminal : ■ 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 de manière adaptative 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. 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.
Limite de début de la charge personnalisée de la batterie principale	Définissez le pourcentage de charge de la batterie qui doit être atteint avant que le terminal démarre la charge de la batterie.
Limite d'arrêt de la charge personnalisée de la batterie principale	Définissez le pourcentage de charge de la batterie qui doit être atteint avant que le terminal arrête la charge de la batterie.

Paramètres	Descriptions
Peak Shift	Sélectionnez **Activer** pour utiliser la fonctionnalité Peak Shift afin de contrôler quand un terminal doit utiliser la charge de la batterie ou le courant alternatif. 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 CA 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 batterie Peak Shift	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	Saisissez une classe et sélectionnez-la dans le menu déroulant. S'affiche après avoir sélectionné **Ajouter des propriétés système**.
Propriété système	Saisissez 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	Saisissez un attribut du BIOS et sélectionnez-le dans le menu déroulant. S'affiche après avoir sélectionné **Ajouter un attribut du BIOS**.

Paramètres	Descriptions
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**.
Package de configuration	Sélectionnez **Importer** pour ajouter le package 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 disposez d'une liste blanche des extensions de fichiers autorisées, vous devez ajouter l'extension de fichier CCTK à cette liste. Naviguez vers **Groupes et paramètres > Tous les paramètres > Contenu > Avancé > Extensions de fichiers** pour ajouter l'extension de fichier.

6 Cliquez sur **Enregistrer et publier**.

Configuration du profil Mises à jour OEM (Windows Desktop)

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**. Pour plus d'informations sur cette page, reportez-vous à Mises à jour des terminaux pour Windows Desktop.

Pour plus d'informations sur les terminaux pris en charge, reportez-vous àChapitre 11 Présentation de Dell Command | Update.

Note Le profil de mises à jour OEM prend en charge les versions 2.4, 3.1 et 3.1.1 de Dell Command | Update. Il ne prend pas en charge la version 3.0.

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 **Mises à jours OEM** et configurez les paramètres suivants :

Paramètres	Description
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**.
Temps	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. Pensez à désactiver des mots de passe du BIOS si vous souhaitez utiliser le profil Mises à jour OEM pour gérer les mises à jour du BIOS. Certaines mises à jour du BIOS demandent à l'utilisateur de saisir le mot de passe du BIOS.
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 périphérique audio fournies par OEM au terminal.

Paramètres	Description
Puce	Sélectionnez **Activer** pour appliquer les mises à jour logicielles du périphérique chipset fournies par OEM au terminal.
Saisie	Sélectionnez **Activer** pour appliquer les mises à jour logicielles du périphérique d'entrée fournies par OEM au terminal.
Réseau	Sélectionnez **Activer** pour appliquer les mises à jour logicielles du périphérique réseau fournies par OEM au terminal.
Stockage	Sélectionnez **Activer** pour appliquer les mises à jour logicielles du périphérique de stockage fournies par OEM au terminal.
Vidéo	Sélectionnez **Activer** pour appliquer les mises à jour logicielles du périphérique vidéo fournies par OEM au terminal.
Autres	Sélectionnez **Activer** pour appliquer les mises à jour logicielles des autres périphériques fournies par OEM au terminal.

6 Cliquez sur **Enregistrer et publier**.

Configurer un profil de kiosque (Windows Desktop)

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**.

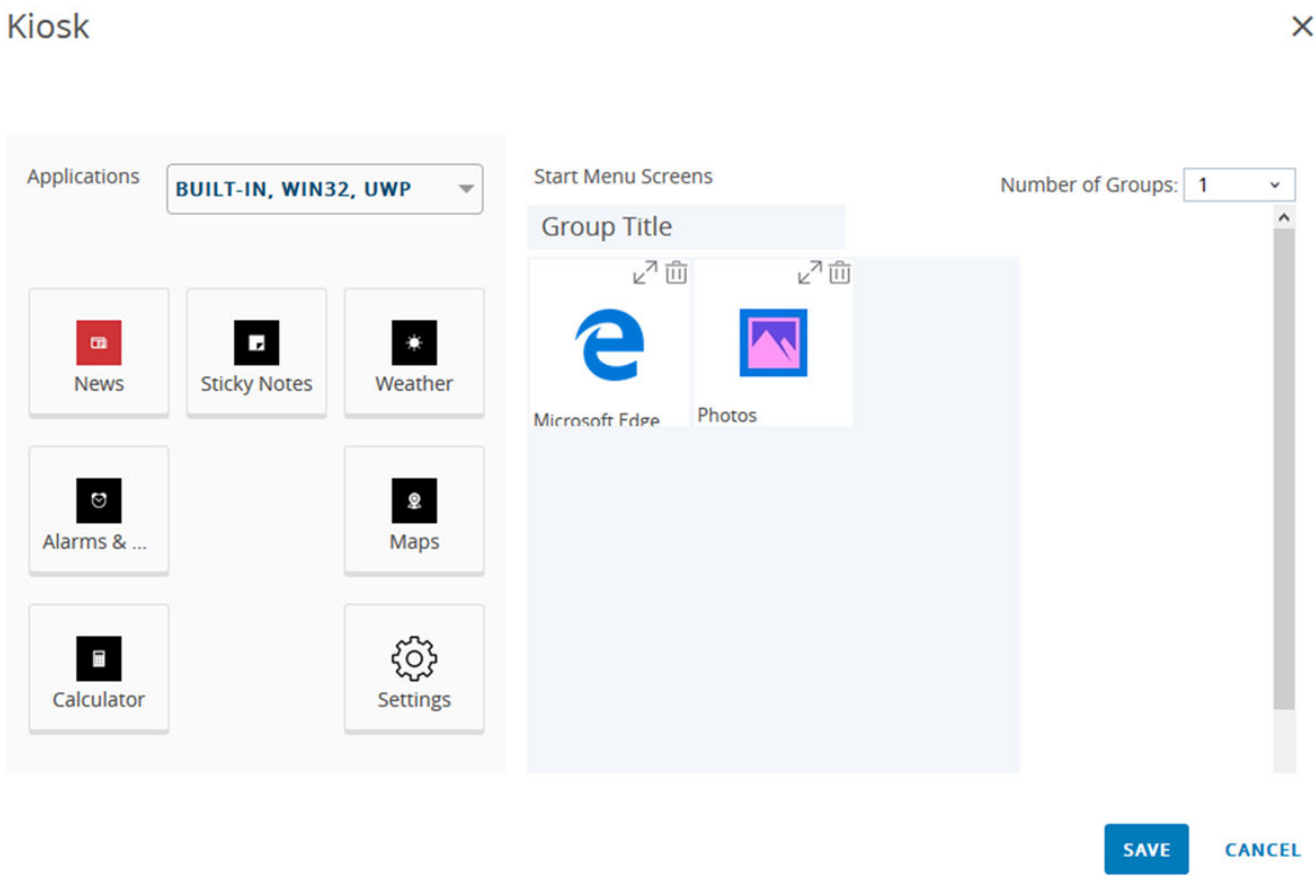
6 Si vous avez déjà votre fichier XML personnalisé, sélectionnez Télécharger le fichier XML du kiosque et complétez les paramètres.

Paramètres	Description
Attribuez 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.

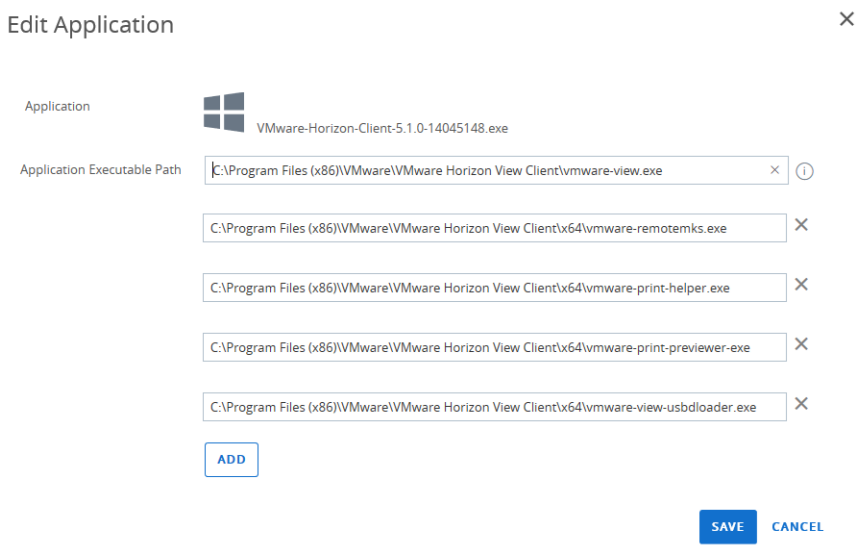
7 Si vous ne disposez pas d'un fichier XML personnalisé, sélectionnez Créer votre kiosque et configurez la disposition de l'application.

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 poste de travail 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**.

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.

Configurer un profil de personnalisation (Windows Desktop)

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. Si vous souhaitez créer un terminal kiosque, reportez-vous à Configurer un profil de kiosque (Windows Desktop).

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 **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**.

Étape suivante

Peer Distribution avec Workspace ONE

Workspace ONE Peer Distribution utilise la fonctionnalité Windows BranchCache native intégrée au système d'exploitation Windows. Cette fonctionnalité fournit aux clients une technologie pair-à-pair pouvant remplacer Adaptiva.

Configurez la distribution pair-à-pair sur vos terminaux Windows 10 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**. Pour plus d'informations, reportez-vous à la section Surveiller votre version d'application individuelle.

Configurer un profil Peer Distribution (Windows Desktop)

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.

Conditions préalables

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. Pour plus d'informations, reportez-vous à la section Configuration requise pour Workspace ONE Peer Distribution.

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 **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**.

Utiliser les paramètres personnalisés (Windows Desktop)

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 section de configuration **Paramètres personnalisés** et le code XML pour activer ou désactiver certains paramètres manuellement.

Conditions préalables

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 simplifier la création du code SyncML, accédez à la page VMware Policy Builder.

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 à la page VMware Policy Builder.

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** et 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 AirWatch Service.

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 `<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**.

Empêcher les utilisateurs de désactiver AirWatch Service

Utilisez un profil de paramètres personnalisés pour empêcher les utilisateurs finaux de désactiver AirWatch Service sur leurs terminaux Windows 10. Empêcher les utilisateurs finaux de désactiver le service AirWatch garantit que Workspace ONE Intelligent Hub exécute des check-ins réguliers avec Workspace ONE UEM Console et reçoit les dernières mises à jour de stratégie.

Procédure

1 Créez un profil **Paramètres personnalisés**. Pour plus d'informations, consultez la section Utiliser les paramètres personnalisés (Windows Desktop).

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="7957d046-7765-4422-9e39-6fd5eef38174">
              <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 pousser 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="7957d046-7765-4422-9e39-6fd5eef38174">
              <parm name="LockDownAwService" value="False"/>
            </characteristic>
          </wap-provisioningdoc>
```

Utilisation de Lignes de base 4

Sécuriser vos terminaux Windows Desktop avec Lignes de base. Workspace ONE UEM regroupe les paramètres recommandés par l'industrie dans une configuration unique pour simplifier la sécurisation de vos périphériques.

La sécurisation de la configuration de vos terminaux selon les meilleures pratiques est un processus chronophage. Workspace ONE UEM regroupe les meilleures pratiques et les paramètres recommandés par le secteur dans des configurations appelées Lignes de base. Ces configurations réduisent considérablement le temps nécessaire à l'installation et à la configuration des terminaux Windows.

Micro-service Cloud

L'option Lignes de base utilise un micro-service Cloud qui gère 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 de terminal.

Tous les terminaux Windows Desktop 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 10 et le serveur DS. Par exemple, si les 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

- Personnalisée : 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. Des stratégies supplémentaires sont ajoutées à votre GPO existant lorsque vous créez une ligne de base personnalisée.
- Évaluations CIS Windows 10 : 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 10.
- Ligne de base de sécurité Windows 10 : 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 pouvez modifier la version du système d'exploitation de toute ligne de base ultérieurement lors de la modification. Pendant la configuration, vous pouvez choisir la ligne de base à utiliser et personnaliser les stratégies de base. Vous pouvez également ajouter toute stratégie supplémentaire dont vous avez besoin dans le cadre du processus de configuration. Ces stratégies sont les stratégies Microsoft ADMX.

Que se passe-t-il après l'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 tous les 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 de check-in 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 désigner 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**. À partir de cette page, vous pouvez modifier et supprimer des lignes de base existantes. Si vous supprimez une ligne de base qui a été transférée vers des terminaux, les paramètres du terminal reviennent aux paramètres avant la publication de la ligne de base 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**.

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. Disponible sur la page **Détails de la ligne de base**, l'état de conformité de la ligne de base s'affiche lorsque les terminaux sont conformes, intermédiaires, non conformes ou non disponibles. L'état de conformité de la ligne de base s'applique uniquement aux lignes de base créées avec l'interface utilisateur.

Note Vous ne pouvez pas voir l'état de conformité des lignes de base personnalisées créées à l'aide de packages ZIP.

Les terminaux **intermédiaires** ont une conformité de 85 à 99 %. Utilisez cette valeur pour déterminer à quel moment la conformité de vos terminaux est insuffisante. 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.

Ce chapitre contient les rubriques suivantes :

Créer une ligne de base

Créez une ligne de base qui configure vos terminaux avec les paramètres et les configurations recommandés par le secteur. Workspace ONE UEM organise Lignes de base en fonction des favoris du secteur, y compris les évaluations du CIS et les lignes de base de sécurité Windows 10 de Microsoft.

Conditions préalables

Les Lignes de base requièrent que les terminaux soient enrôlés dans Workspace ONE UEM et que Workspace ONE Intelligent Hub soit installé.

Si vous publiez une ligne de base personnalisée, 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 l'évaluation CIS ou les lignes de base de sécurité Windows 10, vous n'avez pas besoin d'ajouter ce fichier.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Lignes de base** et sélectionnez **Nouveau**.
2. 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**.

3 Sélectionnez une ligne de base :

Paramètre	Description
Évaluations CIS Windows 10	Cette ligne de base applique les paramètres de configuration proposés par les évaluations CIS. Sélectionnez la version du système d'exploitation et le niveau d'évaluation à appliquer.
Ligne de base de sécurité Windows 10	Cette ligne de base applique les paramètres de configuration proposés par Microsoft. Sélectionnez la version du système d'exploitation 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.

4 Sélectionnez **Suivant**.

5 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.

6 Sélectionnez **Suivant**.

7 Ajoutez des stratégies supplémentaires à la ligne de base. Ces stratégies proviennent de fichiers Microsoft ADMX. Recherchez une stratégie à ajouter et configurez-la.

8 Sélectionnez **Suivant**.

9 Examinez le résumé et sélectionnez **Enregistrer et attribuer**. Le résumé inclut toutes les stratégies personnalisées ou ajoutées.

10 Lors de l'attribution, entrez le Smart Group contenant les terminaux Windows 10 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 d'une attribution précédente, la ligne de base est supprimée du terminal.

Résultats

Workspace ONE UEM attribue la ligne de base à tous les terminaux du Smart Group (outre ces terminaux dans les Smart Groups exclus).

Étape suivante

Vous devez redémarrer le terminal pour que la ligne de base prenne effet.

politiques de conformité

5

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

Pour certaines plateformes, vous pouvez également décider de définir et de mettre en œuvre certaines précautions. Ces précautions incluent le respect des exigences de complexité du mot de passe, 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.

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

Ce chapitre contient les rubriques suivantes :

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 essentiel dans la gestion de l'intégrité 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 ; nous vous recommandons d'examiner le problème. Un état d'avertissement peut avoir plusieurs causes :
  - 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

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

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

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

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

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

Procédure

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

3 Configurez les paramètres d'attestation d'intégrité :

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

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

4 Cliquez sur **Enregistrer**.

Aperçu de l'application Windows Desktop 6

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 VMware Content Locker pour protéger le contenu de l'entreprise sur les terminaux mobiles et déployer VMware Browser afin de garantir une navigation web sécurisée pour vos utilisateurs. Téléchargez Workspace ONE Intelligent Hub pour Windows pour surveiller vos terminaux de manière plus granulaire.

Déployez des applications Win32 sur des terminaux Windows Desktop nécessite la présence d'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.

Ce chapitre contient les rubriques suivantes :

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 en toute sécurité à un catalogue d'applications activé par votre organisation. Une fois l'application configurée à l'aide d'une authentification unique, les utilisateurs n'ont plus besoin de saisir leurs identifiants de connexion au lancement 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. Pour plus d'informations sur Workspace ONE, consultez le document « Setting up the VMware Workspace ONE Application on Devices » disponible dans le Centre de documentation VMware Identity Manager (https://docs.vmware.com).

Configurer Workspace ONE Intelligent Hub pour les terminaux Windows

Workspace ONE Intelligent Hub pour les terminaux Windows est préconfiguré avec AirWatch. Changez ces paramètres lorsque Workspace ONE Intelligent Hub doit répondre à certains besoins de votre entreprise.

Procédure

- Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Windows > Windows Desktop > Paramètres d'Intelligent Hub** pour modifier les paramètres Workspace ONE Intelligent Hub :

  a Configurez les paramètres Workspace ONE Intelligent Hub pour que Workspace ONE Intelligent Hub transmette les données requises à la console AirWatch :

Paramètres	Descriptions
Intervalle d'échantillon de données (min)	Définit les intervalles pendant lesquels Workspace ONE Intelligent Hub récupère des échantillons de données.

  b Configurez les **Paramètres MDM** pour garantir la communication rapide entre le terminal et la console AirWatch.

Paramètres	Descriptions
Sécurité des canaux MDM	Définissez la sécurité de la couche d'application entre le terminal et Workspace ONE UEM Console.

  c Configurez les paramètres **Gestion à distance** pour permettre la communication entre Workspace ONE Intelligent Hub et le serveur de gestion à distance.

Paramètre	Description
Télécharger le cab de gestion à distance	Cliquez sur ce lien pour télécharger le fichier d'installation du cabinet (CAB) pour la gestion à distance de Workspace ONE UEM.
Demander l'autorisation	Activez cette option pour demander à l'utilisateur final d'accepter ou de refuser la demande de gestion à distance de l'administrateur. ■ Saisissez un **Message de demande d'autorisation** qui s'affiche sur le terminal de l'utilisateur après l'envoi d'une demande de gestion à distance. ■ Saisissez le message de **Légende Oui** du bouton d'acceptation de la demande d'autorisation envoyée à l'utilisateur final. ■ Saisissez le message de **Légende Non** du bouton de refus de la demande d'autorisation envoyée à l'utilisateur final.

Étape suivante

Vous pouvez empêcher les utilisateurs finaux de désactiver AirWatch Service sur leurs terminaux à l'aide d'un profil XML personnalisé. Pour plus d'informations, reportez-vous à la section Empêcher les utilisateurs de désactiver AirWatch Service.

Collecter des données à l'aide de Capteurs pour les terminaux Windows Desktop

7

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. Les Capteurs permettent de 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.

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 assure 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 **Capteurs** dans la navigation principale de Workspace ONE UEM Console sous **Ressources**.

Options de Workspace ONE UEM

- Déclencheurs de Capteurs : lors de la configuration de Capteurs, vous pouvez contrôler le moment où le terminal renvoie 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.
- Scripts PowerShell ajoutés : le script PowerShell que vous créez détermine la valeur de chaque capteur. Pour afficher des exemples de scripts qu'il est possible de créer, reportez-vous à Exemples de scripts PowerShell pour Capteurs.

- **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.

  Note 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 de Workspace ONE Intelligence

Si vous utilisez le service Workspace ONE Intelligence, vous pouvez exécuter un rapport ou créer un tableau de bord pour afficher et interagir avec les données de vos Capteurs. 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. Pour plus d'informations sur le travail dans Workspace ONE Intelligence, accédez à Produits VMware Workspace ONE Intelligence.

Ce chapitre contient les rubriques suivantes :

- Exemples de scripts PowerShell pour Capteurs
- Créer un capteur pour les terminaux Windows Desktop

Exemples de scripts PowerShell pour Capteurs

Lorsque vous créez des Capteurs pour les terminaux Windows 10, vous devez charger un script PowerShell ou entrer les commandes PowerShell dans la zone de texte proposée lors de la configuration dans la Workspace ONE UEM Console. Ces commandes renvoient les valeurs des attributs du capteur.

Exemples de scripts PowerShell

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

Note 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_remain
```

- Obtention du numéro de série
  - **Type de valeur** : Chaîne
  - **Contexte d'exécution** : Utilisateur

```
$os=Get-WmiObject Win32_bios -ComputerName $env:computername -ea silentlycontinue
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
  - **Contexte d'exécution** : Administrateur

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

- Vérification du verrouillage du TPM
  - **Type de valeur** : Booléen
  - **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

    - **Contexte d'exécution** : Utilisateur

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

- Vérification de la version BIOS de SMBIOS
    - **Type de valeur** : Booléen
    - **Contexte d'exécution** : Utilisateur

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

- Affichage de l'utilisation moyenne du CPU (%)
    - **Type de valeur** : Entier
    - **Contexte d'exécution** : Utilisateur

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

- Affichage de l'utilisation moyenne de la mémoire
    - **Type de valeur** : 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** : 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** : Entier
  - **Contexte d'exécution** : Utilisateur

```
$Total_bytes=Get-WmiObject -class Win32_PerfFormattedData_Tcpip_NetworkInterface
|Measure-Object -property BytesTotalPersec -Average |Select-Object -ExpandProperty Average
echo ([System.Math]::Round($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 -ExpandProperty
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
  - **Contexte d'exécution** : Utilisateur

```
$chrome = Get-Process chrome -ea SilentlyContinue
          if($chrome){
              echo $true
              }
          else{
              echo $false
              }
```

- Vérification de l'activation du démarrage sécurisé
  - **Type de valeur** : Booléen
  - **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** : 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

- **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 la 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, VMware Workspace ONE Intelligence et Workspace ONE UEM lisent uniquement la première valeur en tant que réponse du script. Si un script renvoie une valeur nulle, VMware Workspace ONE Intelligence et Workspace ONE UEM ne signalent pas le capteur.

Conditions préalables

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 VMware Workspace ONE Intelligence. Pour afficher les données des Capteurs pour un seul terminal, vous n'avez pas besoin de VMware 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** :

Paramètre	Description
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**.

Paramètre	Description
Langue	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** ■ **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.

Étape suivante

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 pour interagir avec les données de plusieurs terminaux.

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

8

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.

Description des Scripts

Les Scripts, situés dans la navigation principale sous **Ressources**, permettent de transférer du code vers des terminaux Windows 10 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 10 à accéder à ce code pour qu'ils puissent l'exécuter sur leurs terminaux lorsque cela est nécessaire. Pour rendre le code disponible, intégrez le Workspace ONE Intelligent Hub aux Scripts de sorte que les utilisateurs puissent accéder au code dans la zone **Applications** du catalogue.

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 la Workspace ONE UEM Console, accédez au groupe organisationnel concerné, sélectionnez **Terminaux > Affichage en liste**, puis choisissez un terminal. 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.

Ce chapitre contient les rubriques suivantes :

- Créer un script pour les terminaux Windows Desktop

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 les Scripts au Workspace ONE Intelligent Hub pour Windows et activez le libre-service aux Scripts pour vos utilisateurs.

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.
Personnalisation du catalogue d'applications	Autorisez l'accès en libre-service aux Scripts dans le catalogue du 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 le 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.

Paramètre	Description
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**. Scripts.

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

Étape suivante

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

Intégration de Dell Command | Configure

9

Intégrez Workspace ONE UEM à Dell Command | Configure pour configurer les paramètres BIOS du terminal. Cette intégration permet d'activer toutes les fonctionnalités du profil BIOS pour les terminaux Windows Desktop.

Notions de base

Intégration de Dell Command | Configure afin d'améliorer la gestion de vos terminaux Dell Enterprise. Si vous souhaitez utiliser la fonctionnalité des modules de configuration du profil BIOS, vous devez ajouter cette intégration à votre environnement.

Terminaux pris en charge

- Ordinateurs de bureau Dell OptiPlex™
- Ordinateurs de bureau et portables Dell Precision Workstation™
- Ordinateurs portables Dell Latitude™

Ajouter Dell Command | Configure à Workspace ONE UEM

Pour intégrer Dell Command | Configure à Workspace ONE UEM, ajoutez le programme en tant qu'application Win32 interne dans Workspace ONE UEM. Pour plus d'informations, reportez-vous à Ajout de Dell Command | Configure à Workspace ONE UEM.

Profil BIOS

Configurez des paramètres BIOS spécifiques sur des terminaux Dell d'entreprise à l'aide d'un profil BIOS. Ces paramètres vous permettent de contrôler la virtualisation matérielle ainsi que la sécurité du BIOS. Pour plus d'informations, consultez la section Configurer un profil BIOS (Windows Desktop).

Ce chapitre contient les rubriques suivantes :

Ajout de Dell Command | Configure à Workspace ONE UEM

Ajoutez Dell Command | Monitor à Workspace ONE UEM Console afin d'améliorer la gestion de vos terminaux Dell Enterprise. Si vous souhaitez utiliser la fonctionnalité des modules de configuration du profil BIOS, vous devez ajouter cette intégration à votre environnement.

Conditions préalables

Vous devez activer la distribution logicielle afin de déployer Dell Command | Configure sur vos terminaux.

Procédure

1. Accédez à https://www.dell.com/support/article/us/en/04/sln311302/dell-command-configure?lang=en et téléchargez la dernière version de Dell Command | Configure.
2. Ouvrez le fichier .EXE, puis cliquez sur **Extraire**. Enregistrez les fichiers extraits dans un dossier.
3. Naviguez vers le dossier et recherchez le fichier .MSI.
4. 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.
5. Dans l'onglet Options de déploiement, définissez les **Privilèges administrateur** sur **Oui**.
6. 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 BIOS sur le terminal.

Intégration de Dell Command | Monitor

10

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. Cette intégration vous permet également de configurer les paramètres BIOS des terminaux.

Notions de base

Intégration de Dell Command | Monitor afin d'améliorer la gestion de vos terminaux Dell Enterprise. Grâce à cette intégration, Workspace ONE UEM indique l'état d'intégrité de la batterie du terminal ainsi que certains paramètres du BIOS.

Terminaux pris en charge

- Ordinateurs de bureau Dell OptiPlex™
- Ordinateurs de bureau et portables Dell Precision Workstation™
- Ordinateurs portables Dell Latitude™
- Ordinateurs portables Dell XPS

Profil BIOS

Configurez des paramètres BIOS spécifiques sur des terminaux Dell d'entreprise à l'aide d'un profil BIOS. Ces paramètres vous permettent de contrôler la virtualisation matérielle ainsi que la sécurité du BIOS. Pour plus d'informations, consultez la section Configurer un profil BIOS (Windows Desktop).

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.

Présentation de Dell Command | Update

11

Dell Command | Update est un logiciel de gestion côté client qui fait partie de la suite Dell Client Command. Le logiciel permet la mise à jour du microprogramme, des pilotes et des applications pour les terminaux Dell pris en charge.

Notions de base

Intégrez Dell Command | Update afin d'améliorer la gestion des mises à jour de vos terminaux Dell Enterprise. Avec cette intégration, Workspace ONE UEM prend en charge la mise à jour à distance du microprogramme, des pilotes et des autres applications. Vous pouvez contrôler le moment et le type des mises à jour à déployer vers les terminaux.

Terminaux pris en charge

- Ordinateurs de bureau Dell OptiPlex™
- Ordinateurs de bureau et portables Dell Precision Workstation™
- Ordinateurs portables Dell Latitude™

Ajout de Dell Command | Update à Workspace ONE UEM

Pour intégrer Dell Command | Update à Workspace ONE UEM, ajoutez l'application en tant qu'application Win32 interne dans Workspace ONE UEM Console. Pour plus d'informations, consultez la section Ajout de Dell Command | Update à Workspace ONE UEM.

Configuration du profil Mises à jour OEM

Configurez le profil Mises à jour OEM pour activer Dell Command | Update sur les terminaux des utilisateurs finaux. Pour plus d'informations, consultez la section Configuration du profil Mises à jour OEM (Windows Desktop).

Ce chapitre contient les rubriques suivantes :

Ajout de Dell Command | Update à Workspace ONE UEM

Pour améliorer la gestion de vos terminaux Dell Enterprise, ajoutez Dell Command | Update dans Workspace ONE UEM Console. Le profil Mises à jour OEM requiert cette application avant tout déploiement sur les terminaux.

Conditions préalables

Vous devez activer la distribution logicielle afin de déployer Dell Command | Update sur vos terminaux.

Procédure

1. Accédez à http://en.community.dell.com/techcenter/enterprise-client/w/wiki/7534.dell-command-update et téléchargez la dernière version de Dell Command | Update.
2. Dans UEM Console, ajoutez le fichier EXE 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.
3. Dans l'onglet Options de déploiement, définissez les **Privilèges administrateur** sur **Oui**.
4. 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

12

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

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

Ce chapitre contient les rubriques suivantes :

Tableau de bord des terminaux

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

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

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

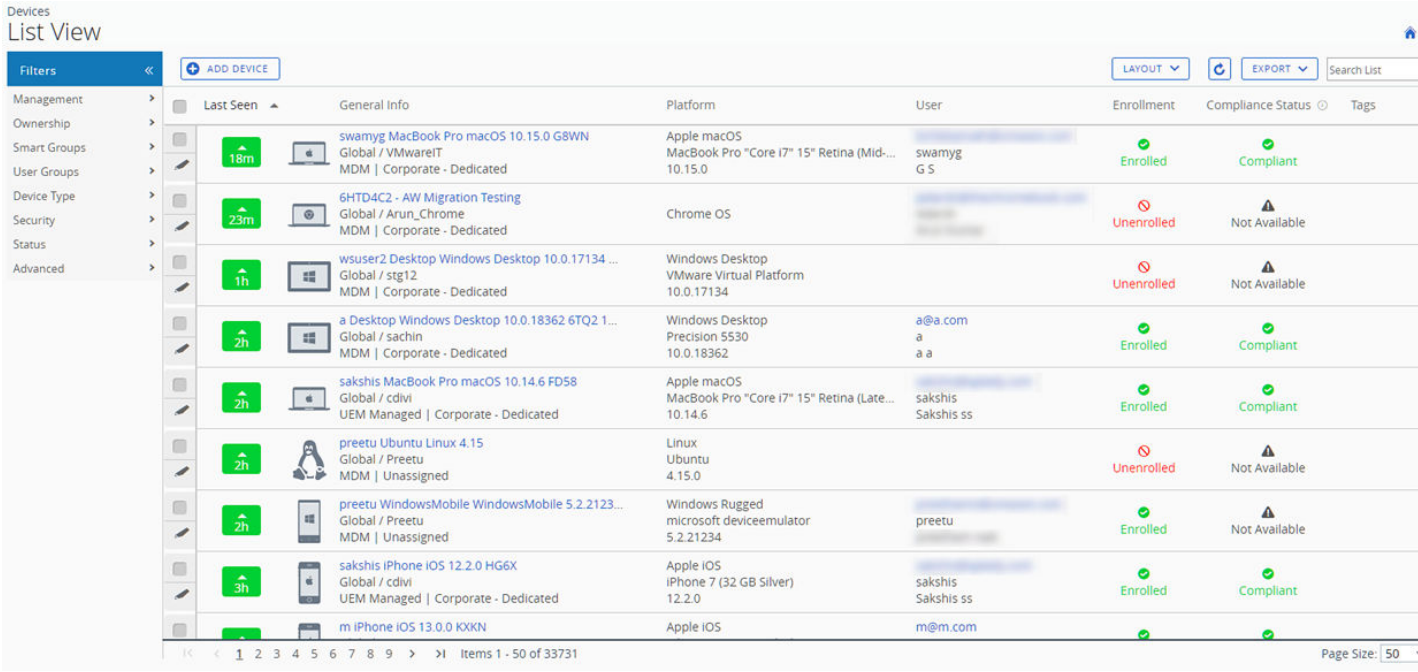
À partir de cet **affichage en liste**, vous pouvez effectuer des actions administratives : envoyer un message, verrouiller ou supprimer des terminaux et modifier les groupes associés à un terminal.

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

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

Affichage en liste des terminaux

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



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

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

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

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

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

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

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

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

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

Exporter l'affichage en liste

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

Recherche dans l'affichage en liste des terminaux

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

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

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

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

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

Assistance à distance

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

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

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

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

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

Détails de la page Terminal Windows Desktop

Utilisez la page Détails dans Workspace ONE UEM powered by AirWatch 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 un 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.

Dans la page Détails du terminal, vous pouvez accéder aux informations propres aux terminaux, réparties dans différents onglets de menu. Chaque onglet de menu contient des informations relatives aux terminaux en fonction de votre déploiement Workspace ONE UEM.

Détails du service de notification Windows

Vous pouvez voir l'état de la communication du terminal avec le service de notification Windows (WNS) dans l'onglet Réseau de la page Détails du terminal. WNS prend en charge l'envoi des notifications de votre terminal. 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.

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). Pour plus d'informations sur WNS, consultez https://docs.microsoft.com/en-us/windows/client-management/mdm/push-notification-windows-mdm.
- **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 en fonction des facteurs, tels que les paramètres de Workspace ONE UEM Console ou l'état 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.
- **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 une action en masse à l'aide de la méthode de sélection de bloc (en utilisant la touche Maj) au lieu de sélectionner la case principale (en regard de l'en-tête de la colonne Dernière connexion visible dans la vue de la liste des terminaux).

- **Modifier le 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 l'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.

  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.

- **Envoyer une requête à tous les terminaux** – Envoyez une commande de requête au terminal pour recevoir une liste des applications (dont Workspace ONE Intelligent Hub, le cas échéant), des livres, des certificats, des informations sur le terminal, des profils et des mesures de sécurité installés.
- **Redémarrer le terminal** – Redémarrez un terminal à distance.
- **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 le Workspace ONE Intelligent Hub sur les terminaux Windows 10 pour rétablir la communication entre la console et le terminal.

  Certains événements peuvent affecter la communication entre le terminal et la console. Certains exemples entraînent l'arrêt des services Workspace ONE UEM clés, la suppression ou la corruption des fichiers associés au Workspace ONE Intelligent Hub et l'échec des mises à niveau des composants du 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.
- **Demande du journal du terminal** – Demandez le journal de débogage du terminal sélectionné. Vous pouvez ensuite afficher le journal en sélectionnant l'onglet **Plus** et en cliquant sur **Pièces jointes > Documents**. Vous ne pouvez pas afficher le journal dans Workspace ONE UEM Console. Le journal est fourni sous la forme d'un fichier Zip qui peut être utilisé pour le dépannage et l'assistance.

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

- **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**.

Workspace ONE Assist

Workspace ONE Assist (anciennement ARM, pour Advanced Remote Management) vous permet de vous connecter à distance aux terminaux des utilisateurs finaux à des fins de résolution de problèmes et de maintenance. Le serveur d'assistance facilite la communication entre Workspace ONE UEM powered by AirWatch et le terminal « hôte ».

Pour plus d'informations, reportez-vous à la section **Documentation relative à VMware Workspace ONE Assist** sur docs.vmware.com.

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.

Préparer vos terminaux HoloLens pour la gestion de Workspace ONE UEM

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 de licences, reportez-vous à la documentation https://docs.microsoft.com/en-us/hololens/hololens1-upgrade-enterprise. 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 10 natives, car les terminaux HoloLens ne prennent pas en charge la fonctionnalité Workspace ONE Intelligent Hub. Pour plus d'informations, reportez-vous à Enrôlement MDM natif pour Windows Desktop.

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 obtenir la liste des CSP pris en charge, reportez-vous à la documentation https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference#hololens.

Aperçu de la configuration de produits

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 UEM Console. Créez ces serveurs pour chaque stock ou entrepôt afin de stocker le contenu de produits destinés à être distribués sur vos terminaux.

Pour plus d'informations, reportez-vous à la documentation Provisionnement de produit.