Gestion de la messagerie mobile

VMware Workspace ONE UEM

vmware by Broadcom

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

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

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

Table des matières

Qu'est-ce que la solution de gestion de la messagerie mobile de Workspace ONE UEM ?

1

La possibilité de consulter les données professionnelles sur votre terminal vous permet d'augmenter votre productivité. Cependant, cette possibilité comporte également des risques en termes de sécurité et de déploiement. Pour relever ces défis, la solution de Workspace ONE UEM powered by AirWatch Gestion de la messagerie mobile (MEM) protège votre infrastructure de messagerie professionnelle dans son intégralité. Utilisez Workspace ONE UEM powered by AirWatch pour gérer votre déploiement de messagerie mobile.

La possibilité de consulter les données professionnelles sur votre terminal vous permet d'augmenter votre productivité. Cependant, cette possibilité comporte également des risques en termes de sécurité et de déploiement. Pour relever ces défis, la solution de Workspace ONE UEM powered by AirWatch Gestion de la messagerie mobile (MEM) protège votre infrastructure de messagerie professionnelle dans son intégralité.

Défis

La messagerie mobile offre des avantages et présente simultanément de plus grands défis, notamment :

- Le provisionnement de la messagerie à travers différents types de terminaux, systèmes d'exploitation et clients de messagerie
- La protection de l'accès à la messagerie sur des réseaux non sécurisés
- La protection d'informations sensibles depuis des applications tierces
- L'interdiction d'accéder à la messagerie depuis des terminaux volés ou perdus
- L'impossibilité de perdre ou de diffuser les pièces jointes à travers les applications de lecture tierces lorsqu'elles s'affichent.

Avantages de la solution de gestion de la messagerie mobile (MEM)

Workspace ONE UEM powered by AirWatch MEM vous fournit tous les facteurs clés nécessaires pour un déploiement de messagerie mobile sûr et réussi. L'utilisation de MEM présente de nombreux avantages, notamment :

- Appliquer la sécurité SSL

- Configurer la messagerie à distance
- Détecter les terminaux non gérés existants
- Protéger les e-mails contre la perte de données
- Empêcher les terminaux non gérés d'accéder aux e-mails
- Bloquer l'accès à la messagerie pour les terminaux approuvés par l'entreprise uniquement
- Utiliser la révocation et l'intégration des certificats

Configuration MEM requise

Vérifiez les conditions du navigateur, comme indiqué dans cette section avant de continuer à utiliser la solution VMware AirWatch® Mobile Email Management® (MEM).

Exclusion

L'intégration avec un produit tiers n'est pas garantie et dépend du bon fonctionnement de ces solutions tierces.

Navigateurs pris en charge

La console Workspace ONE UEM prend en charge les derniers builds stables des navigateurs Internet suivants :

- Chrome
- Firefox
- Safari
- Internet Explorer 11
- Microsoft Edge

Note Si vous utilisez IE pour accéder à la console UEM, accédez à **Panneau de contrôle > Paramètres > Options Internet > Sécurité** et assurez-vous que le niveau de sécurité ou le niveau de sécurité personnalisé inclut l'option **Téléchargement des polices**, et que cette dernière est définie sur **Activé**.

Si vous utilisez un navigateur antérieur à ceux répertoriés ci-dessus, mettez à jour votre navigateur pour pouvoir accéder à toutes les fonctionnalités de la console Workspace ONE UEM. Des tests approfondis ont été effectués sur plusieurs plateformes afin de garantir le bon fonctionnement de ces navigateurs Internet. UEM Console peut rencontrer quelques problèmes mineurs si vous optez pour un navigateur non certifié.

Modèles de déploiement pour la gestion de l'infrastructure de messagerie

2

Pour protéger et gérer votre infrastructure de messagerie, Workspace ONE UEM propose deux types de modèles de déploiement : le modèle proxy et le modèle direct.

Vous pouvez utiliser le modèle de votre choix de déploiement de messagerie, ainsi que les stratégies de messagerie que vous définissez dans la console UEM pour gérer efficacement vos terminaux mobiles.

- Avec le modèle de déploiement de proxy, un serveur à part appelé serveur proxy Secure Email Gateway (SEG) est placé entre le serveur Workspace ONE et le serveur de messagerie d'entreprise. Ce serveur proxy filtre toutes les requêtes des terminaux au serveur de messagerie et relaie le trafic des terminaux approuvés uniquement. Le serveur de messagerie d'entreprise est ainsi protégé, car il ne communique pas directement avec les terminaux mobiles.
- Avec le modèle de déploiement direct, aucun serveur proxy n'est impliqué et Workspace ONE UEM communique directement avec les serveurs de messagerie. L'absence de serveur proxy simplifie les étapes de configuration et d'installation avec ce modèle.

Note Le modèle de déploiement de proxy dispose de deux variantes : les plates-formes classique et SEG v2. La plate-forme SEG classique n'est plus prise en charge, car la plate-forme SEG v2 garantit de meilleures performances sur la plate-forme classique. La plate-forme SEG v2 peut être installée sur un serveur SEG existant avec une interruption de service minimale et lors d'une mise à niveau. Aucune modification de profil ou interaction d'utilisateur final n'est requise.

Modèle de déploiement	Mode de configuration	Infrastructure de messagerie
Modèle de déploiement de proxy	Microsoft Exchange 2010/2013/2016 Exchange Office 365	Microsoft Exchange 2010/2013/2016/2019 Exchange Office 365 HCL Domino avec HCL Gmail
Modèle de déploiement direct – PowerShell	Modèle PowerShell	Microsoft Exchange 2010/2013/2016/2019 Microsoft Office 365
Modèle de déploiement direct - Gmail	Gmail	

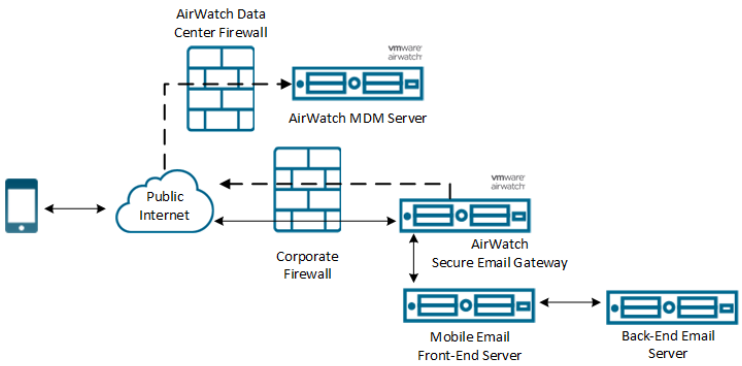
Note Workspace ONE UEM ne prend en charge que les versions des serveurs de messagerie tiers supportées par le fournisseur de serveurs de messagerie. Lorsque le fournisseur déconseille une version de serveur, Workspace ONE UEM ne prend plus en charge l'intégration avec cette version obsolète.

Modèle de proxy SEG (Secure Email Gateway)

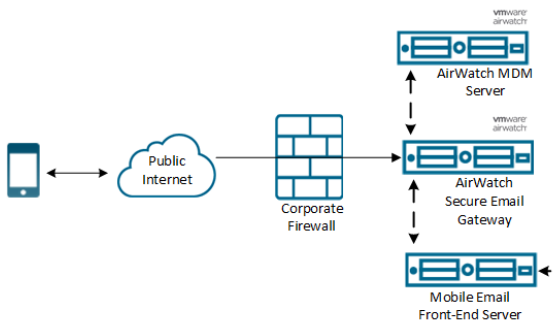
Le serveur proxy Secure Email Gateway (SEG) est un serveur à part installé avec votre serveur de messagerie existant pour proxifier tout le trafic de messagerie destiné aux terminaux mobiles. En fonction des paramètres définis dans UEM Console, le serveur proxy SEG prend des décisions d'autorisation ou de blocage pour chaque terminal qu'il gère.

Le serveur proxy SEG filtre toutes les requêtes de communication au serveur de messagerie et relaie le trafic des terminaux approuvés uniquement. Ce relais protège la messagerie professionnelle en n'autorisant pas tous les terminaux à communiquer avec lui.

Installez le serveur SEG sur votre réseau afin qu'il s'aligne sur le trafic de messagerie de l'entreprise. Vous pouvez aussi l'installer dans une DMZ ou derrière un proxy inverse. Vous devez héberger le serveur SEG dans votre centre de données, que votre serveur Workspace ONE MDM soit sur site ou dans le Cloud.



Cloud Architecture

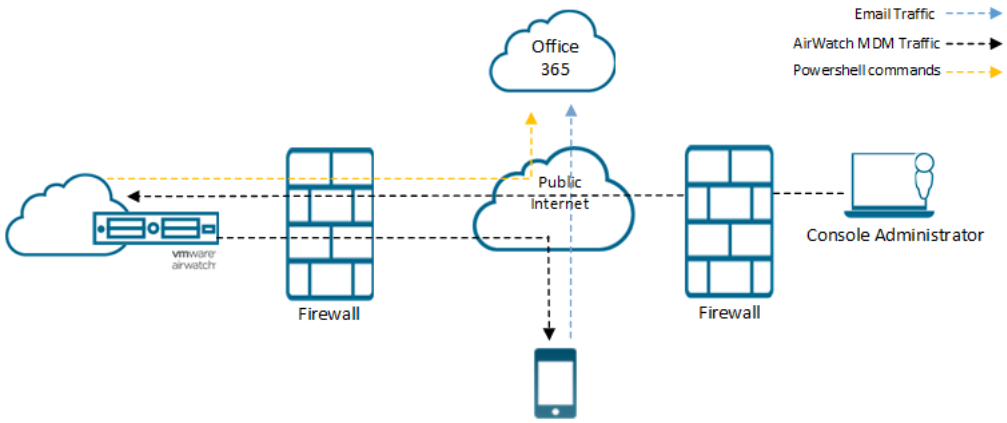


On-premise Architecture

Déploiement direct du modèle PowerShell

Dans le modèle PowerShell, Workspace ONE UEM remplit un rôle d'administrateur PowerShell et émet des commandes vers l'infrastructure Exchange ActiveSync (EAS) pour autoriser ou interdire l'accès aux e-mails selon les stratégies définies dans UEM console. Les déploiements PowerShell ne nécessitent pas de serveur proxy de messagerie et le processus d'installation est plus simple.

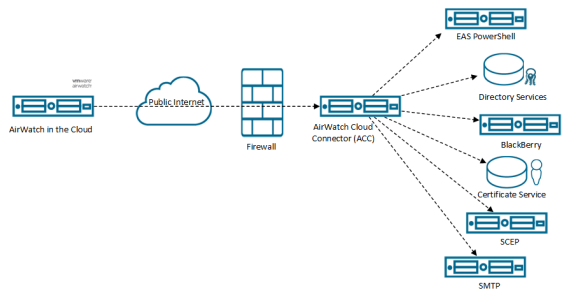
Les déploiements PowerShell sont adaptés aux entreprises qui utilisent Microsoft Exchange 2010, 2013, 2016, 2019 ou Office 365.



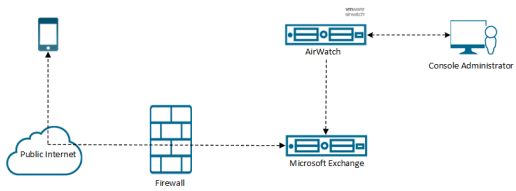
Microsoft Office 365

Il existe deux façons selon lesquelles les commandes PowerShell sont émises en fonction de l'emplacement du serveur Workspace ONE UEM et du serveur Exchange :

- Le serveur Workspace ONE se trouve dans le Cloud et le serveur Exchange sur site – Le serveur Workspace ONE UEM émet les commandes PowerShell. VMware Enterprise Systems Connector configure la session PowerShell avec le serveur de messagerie.
- Le serveur Workspace ONE UEM et le serveur de messagerie se trouvent sur le site – Le serveur Workspace ONE UEM configure la session PowerShell directement avec le serveur de messagerie. Ici, aucun serveur VMware Enterprise Systems Connector n'est nécessaire sauf si le serveur Workspace ONE UEM ne peut pas communiquer directement avec le serveur de messagerie.



Microsoft Exchange 2010 with AirWatch Cloud



Microsoft Exchange 2010 with AirWatch On-Prem

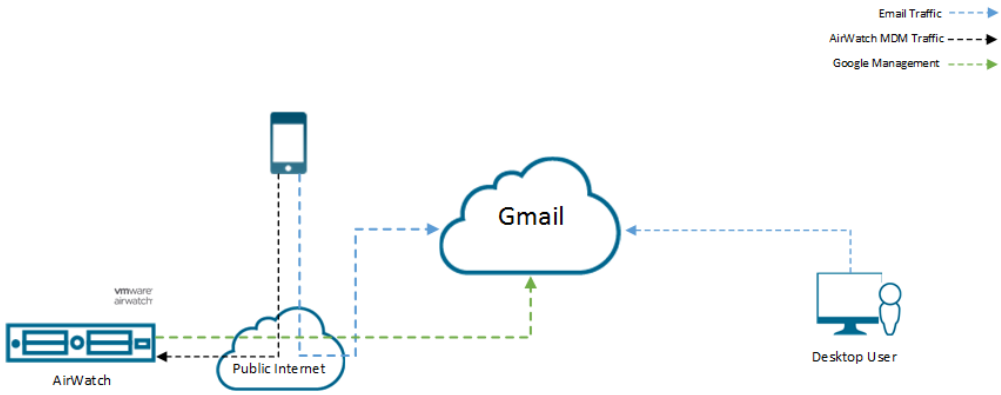
Pour vous aider à choisir entre les modèles de déploiement Secure Email Gateway et PowerShell, reportez-vous à la section Recommandations Workspace ONE UEM.

Modèle direct Gmail

Intégrez un serveur Workspace ONE UEMavec Google.

Les organisations qui utilisent l'infrastructure de messagerie Gmail connaissent peut-être déjà les défis posés par la protection des terminaux de la messagerie pour Gmail et la difficulté d'empêcher le contournement du terminal sécurisé. Workspace ONE UEM répond à ces problématiques en fournissant une approche flexible et sûre pour intégrer votre infrastructure de messagerie.

Dans le modèle de déploiement direct de Gmail, le serveur Workspace ONE UEM communique directement avec Google. En fonction des besoins de sécurité, Workspace ONE peut gérer le mot de passe Google d'un utilisateur et contrôler l'accès à la boîte de réception de l'utilisateur.



Appels d'API à Google Suite : vous pouvez personnaliser les attributs utilisés dans les appels d'API à Google Suite en spécifiant un autre attribut au lieu de l'adresse e-mail de l'utilisateur. Par défaut, l'adresse e-mail de l'utilisateur est utilisée. Pour plus d'informations sur la manière de configurer le modèle direct de Gmail, reportez-vous à la section *Intégrer le modèle direct avec la gestion de mot de passe*.

Matrice de modèles de déploiement MEM

Utilisez la matrice ci-dessous pour comparer les fonctionnalités disponibles dans les différents modèles de déploiement MEM.

Office 365 requiert une configuration supplémentaire pour le modèle de proxy SEG. Workspace ONE UEM recommande le modèle d'intégration direct pour les serveurs basés dans le Cloud. Reportez-vous à la section Recommandations Workspace ONE UEM pour plus de détails.

✓	Pris en charge	□	Non supporté par Workspace ONE UEM
X	Fonctionnalité non disponible	N/A	Non applicable

Tableau 2-1. Matrice de déploiement

	Modèle de proxy SEG			Modèle direct		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365 (PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Outils de sécurité des e-mails						
Paramètres de sécurité appliqués						
Utiliser les signatures numériques avec la fonctionnalité S/MIME	✓	□	□	✓	✓	N/A
Protéger les données sensibles par le chiffrement forcé	✓	✓	✓	✓	✓	✓
Appliquer la sécurité SSL	✓	✓	✓	✓	✓	✓
Sécurité des pièces jointes et des liens hypertexte						
Appliquer les pièces jointes et liens hypertextes dans VMware AirWatch Content Locker ou Workspace ONE Web uniquement	✓	✓	✓	x	x	x
Configuration automatique de la messagerie						
Configurer les e-mails à distance sur le terminal	✓	✓	✓	✓	✓	✓

Tableau 2-1. Matrice de déploiement (suite)

	Modèle de proxy SEG			Modèle direct		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365 (PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Contrôle de l'accès à la messagerie						
Empêcher les terminaux non gérés d'accéder aux e-mails	✓	✓	✓	✓	✓	✓
Détecter les terminaux non gérés existants	✓	✓	✓	✓	✓	N/A
Accès à la messagerie sans politique de conformité personnalisable	✓	✓	✓	✓	✓	✓
Demander le chiffrement du terminal pour accéder à la messagerie	✓	✓	✓	✓	✓	✓
Empêcher les terminaux compromis d'accéder à la messagerie	✓	✓	✓	✓	✓	✓
Autoriser/ bloquer la messagerie - Client de messagerie	✓	✓	✓	✓	✓	x
Contrôle de l'accès à la messagerie						
Autoriser/ bloquer la messagerie - Utilisateur	✓	✓	✓	✓	✓	x

Tableau 2-1. Matrice de déploiement (suite)

	Modèle de proxy SEG			Modèle direct		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365 (PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Autoriser/ bloquer la messagerie - Modèle du terminal	✓	✓	✓	✓	✓	✓
Autoriser/ bloquer la messagerie - OS du terminal	✓	✓	✓	✓	✓	✓
Autoriser/ bloquer la messagerie - Type de terminal EAS	✓	✓	✓	✓	✓	x
Visibilité de la gestion						
Statistiques du trafic de messagerie	✓	✓	✓	x	x	x
Statistiques du client de messagerie	✓	✓	✓	x	x	x
Gestion des certificats						
Intégration/ Révocation de la CA	✓	□	□	✓	✓	N/A
Architecture						
Passerelle intégrée (proxy)	✓	✓	✓	N/A	N/A	✓
Exchange PowerShell	N/A	N/A	N/A	✓	✓	N/A
Gestion de mot de passe pour Gmail	N/A	N/A	✓	N/A	N/A	✓
Intégration des API d'annuaire pour Gmail	N/A	N/A	N/A	N/A	N/A	✓
Pris en charge						

Tableau 2-1. Matrice de déploiement (suite)

	Modèle de proxy SEG			Modèle direct		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365 (PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Workspace ONE Boxer pour iOS et Android [^]	✓	✓	✓	✓	✓	✓
Client de messagerie natif iOS	✓	✓	✓	✓	✓	✓
Client de messagerie native Android (Gmail)	✓	✓	✓	✓	✓	✓
Client Android HCL Notes*	N/A	✓	N/A	N/A	N/A	N/A

*La sécurité des pièces jointes et des liens hypertexte n'est pas prise en charge pour les clients Android HCL Notes.

+ Exchange 2003 n'est pas pris en charge.

^ Exchange 2003, les stratégies de chiffrement et les déploiements MEM multiples ne sont pas pris en charge pour Workspace ONE Boxer.

Recommandations de Workspace ONE UEM

Les fonctionnalités prises en charge par Workspace ONE UEM et les tailles de déploiement appropriées sont répertoriées dans cette section. Utilisez la matrice de décision afin de choisir le déploiement qui répond le mieux à vos besoins.

Chiffrement des pièces jointes

Grâce au chiffrement appliqué sur les pièces jointes de vos terminaux mobiles, Workspace ONE UEM assure leur sécurité sans altérer l'expérience de l'utilisateur.

	Applications natives	Traveler	Workspace ONE Boxer
iOS	✓		
Android	✓		
SEG prend en charge le chiffrement des pièces jointes et la transformation des liens hypertexte sur Workspace ONE Boxer dans la mesure où ces fonctionnalités sont activées pour la configuration de l'application Boxer dans la console UEM. SEG prend en charge le chiffrement des pièces jointes avec Exchange 2010/2013/2016/2019 et Office 365.			

Note SEG ne chiffre pas les pièces jointes pour Workspace ONE Boxer, mais le DLP peut être appliqué au niveau de l'application.

Gestion d'e-mails

Cette liste vous offre le niveau de sécurité le plus élevé avec la gestion et le déploiement les plus simples.

Infrastructure d'e-mails	Gmail	PowerShell	Secure Email Gateway (SEG)
Infrastructure de messagerie Cloud			
Office 365		✓	✓
Gmail	✓		✓
Infrastructure de messagerie sur site			
Exchange 2010		✓	✓
Exchange 2013		✓	✓
Exchange 2016		✓	✓
Exchange 2019		✓	✓
HCL Notes			✓

^Utilisez Secure Email GatewaySecure Email Gateway (SEG) pour toutes les infrastructures de messagerie comprenant des déploiements supérieurs à 100 000 terminaux. Pour les déploiements inférieurs à 100 000 terminaux, vous pouvez utiliser PowerShell pour gérer votre messagerie. Reportez-vous à la section Matrice de décisions Secure Email Gateway vs PowerShell.

**Le seuil pour les installations PowerShell est basé sur les derniers tests de performances effectués et peut varier selon les versions disponibles. Les déploiements de 50 000 terminaux maximum peuvent bénéficier d'un temps relativement court de synchronisation et d'exécution de la conformité (moins de trois heures). Pour les déploiements qui s'approchent des 100 000 terminaux, les administrateurs doivent envisager un temps des processus de synchronisation et d'exécution de la conformité plus important, entre 3 et 7 heures.

Matrice de décisions Secure Email Gateway vs PowerShell

Cette matrice vous présente les fonctionnalités de déploiement de SEG et de PowerShell pour vous aider à choisir le déploiement qui répond à vos besoins.

	Avantages	Inconvénients
SEG	■ Conformité en temps réel ■ Chiffrement des pièces jointes ■ Transformation des liens hypertexte	■ Serveur(s) supplémentaire(s) requis
PowerShell	■ Aucun serveur sur site requis pour la gestion de la messagerie ■ Le trafic de messagerie n'est pas routé vers un serveur sur site avant d'être dirigé vers Office 365. ADFS n'est donc pas obligatoire	■ Aucune synchronisation de conformité en temps réel ■ Pas pour les déploiements importants (supérieurs à 100 000 terminaux)
Microsoft suggère l'utilisation d'Active Directory Federated Services (ADFS) pour empêcher l'accès direct aux comptes de messagerie Office 365.		

Migrer votre infrastructure de messagerie vers Workspace ONE UEM

3

Vous pouvez migrer votre adresse e-mail vers un modèle de gestion de la messagerie mobile (MEM) avec Workspace ONE UEM. En migrant vers l'un de ces modèles EME, vous pouvez appliquer les politiques de contrôle d'accès à la messagerie permettant d'assurer que seuls les utilisateurs et les terminaux approuvés accèdent aux e-mails :

- Secure Email Gateway (SEG)
- PowerShell
- Gmail

Migrer vers Secure Email Gateway (SEG)

La migration de la messagerie vers Secure Email Gateway (SEG) permet aux utilisateurs d'accéder à leurs e-mails uniquement via le proxy SEG.

Utiliser SEG permet d'appliquer les stratégies de contrôle d'accès à la messagerie, afin que seuls les terminaux et utilisateurs approuvés bénéficient de l'accès. Les politiques de chiffrement des pièces jointes garantissent la sécurité des données.

1 Configurez SEG pour le groupe organisationnel nécessaire sous Global dans Workspace ONE UEM Console. .

2 Téléchargez et installez SEG..

3 Testez la fonctionnalité SEG à l'aide de la politique de conformité de la messagerie.

   a Désactivez temporairement toutes les stratégies de conformité.

   b Demandez à tous les utilisateurs d'enrôler leurs terminaux dans Workspace ONE UEM.

   c Provisionnez un nouveau profil de messagerie (avec l'URL du serveur SEG comme nom d'hôte) pour tous les terminaux enrôlés.

   d Rappelez régulièrement aux utilisateurs de terminaux non gérés de s'enrôler dans Workspace ONE UEM.

   e Pour bloquer l'accès EAS au serveur de messagerie à une date précise, modifiez les règles du pare-feu (ou de la passerelle de gestion des menaces). Ceci permet de s'assurer que les terminaux ne peuvent pas accéder directement au serveur de messagerie.

f Activez toutes les politiques de conformité.

Note Le Webmail existant, Outlook Web Access (OWA) et les autres clients de messagerie continuent d'accéder au serveur de messagerie.

Migrer vers PowerShell

Vous pouvez sécuriser vos terminaux et synchroniser les terminaux avec Exchange ou Office 365 pour les e-mails en migrant vers PowerShell.

L'environnement PowerShell détecte les terminaux gérés et non gérés, et grâce aux stratégies de contrôle d'accès à la messagerie, il donne accès aux terminaux et aux utilisateurs approuvés uniquement.

1 Configurez l'intégration de PowerShell pour le groupe organisationnel nécessaire sous Global dans la console Workspace ONE UEM.

2 Configurez l'intégration avec les groupes d'utilisateurs (personnalisés ou prédéfinis).

3 Testez la fonctionnalité PowerShell avec un sous-ensemble d'utilisateurs (par exemple, des utilisateurs test) pour vous assurer que les éléments suivants fonctionnent :

   a Synchronisation avec le serveur de messagerie pour identifier les terminaux.

   b Contrôle d'accès en temps réel.

4 Désactivez temporairement toutes les stratégies de conformité.

5 Fournissez un nouveau profil de messagerie à tous les terminaux enrôlés dans Workspace ONE UEM avec le nom d'hôte du serveur de messagerie.

6 Procédez à la synchronisation avec le serveur de messagerie pour détecter tous les terminaux (gérés ou non) qui synchronisent leur messagerie.

7 Rappelez régulièrement aux utilisateurs de terminaux non gérés de s'enrôler dans Workspace ONE UEM.

8 Activez et appliquez les règles de conformité pour bloquer l'accès à la messagerie, à une date précise, pour tous les terminaux non conformes, notamment les terminaux non gérés.

9 Configurez le serveur de messagerie pour bloquer tous les terminaux par défaut.

Note Le Tableau de bord des e-mails affiche la liste des terminaux non gérés en tant que terminaux bloqués et gérés qui sont autorisés pour la messagerie.

Intégrer Gmail avec Workspace ONE UEM

En migrant vers Gmail, vous pouvez synchroniser vos terminaux avec le serveur Gmail. Vous pouvez intégrer Gmail avec ou sans Secure Email Gateway (SEG), ou directement avec les API d'annuaire.

1 Activez l'authentification unique (SSO) sur Gmail ou créez un certificat de compte de service.

2 Configurez l'intégration de Gmail depuis Workspace ONE UEM Console à l'aide de l'assistant de configuration MEM.

3 Provisionnez les profils EAS pour les utilisateurs avec le nouveau mot de passe aléatoire. Les terminaux ne recevant pas ce profil voient leur accès à Gmail automatiquement bloqué.

Migrer les terminaux

Vous pouvez migrer des terminaux à travers des groupes organisationnels et des déploiements MEM avec Workspace ONE UEM.

1 Dans Workspace ONE UEM Console, accédez au **Tableau de bord des e-mails**.

2 Filtrez les terminaux gérés qui se trouvent sous votre déploiement MEM actuel.

3 Sur la page d'**affichage en liste**, sélectionnez tous les terminaux, puis **Administration > Migrer les terminaux** dans le menu déroulant.

4 Sur la page **Confirmation de la migration de terminaux**, saisissez le code donné pour confirmer la migration et sélectionnez la configuration pour le déploiement de vos terminaux.

5 Cliquez sur **Continuer**.

Résultat

Une fois ces étapes suivies, Workspace ONE UEM supprime automatiquement le profil Exchange ActiveSync (EAS) précédent et transmet le nouveau profil EAS avec le groupe de déploiement cible. Le terminal se connecte alors à son nouveau groupe de déploiement. Le nom de configuration MEM mis à jour pour le terminal s'affiche sur le tableau de bord des e-mails.

Configuration du déploiement de solution de gestion de la messagerie mobile (MEM)

4

Intégrez votre infrastructure de messagerie en quelques étapes grâce à l'assistant de configuration MEM. MEM ne peut être configuré qu'en tant que groupe organisationnel parent et ne peut pas être remplacé par un groupe organisationnel enfant.

Une configuration MEM peut être associée à un ou plusieurs profils Exchange ActiveSync (EAS).

1 Naviguez vers **Email** > **Paramètres** et sélectionnez **Configurer**.

2 Choisissez le modèle de déploiement, puis sélectionnez le type de serveur de messagerie. Sélectionnez **Suivant**.

   a Si le modèle de déploiement choisi est Proxy, sélectionnez le type de messagerie.

   Les choix sont les suivants :

   - Exchange
   - Google
   - HCL Notes

   b Si le modèle de déploiement choisi est Direct, sélectionnez le type de messagerie.

   Les choix sont les suivants :

   - Exchange
   - Google Apps avec l'API direct
   - Google Apps avec le provisionnement de mot de passe - Sélectionnez Avec rétention du mot de passe ou Sans rétention du mot de passe comme type de déploiement Gmail.

   Pour plus d'informations sur les méthodes de déploiement, consultez la section Types de déploiement de messagerie.

3 Entrez les détails pour le type de déploiement choisi.

   Les choix sont les suivants :

   - Pour les déploiements SEG :
     1 Saisissez un nom convivial pour ce déploiement.
     2 Saisissez les détails du serveur proxy SEG.

- Pour les déploiements PowerShell :
  1. Saisissez un nom convivial pour ce déploiement.
  2. Saisissez les détails du serveur PowerShell, le mode d'authentification, et synchronisez les paramètres.
- Pour Gmail :
  1. Saisissez un nom convivial pour ce déploiement.
  2. Saisissez les détails des paramètres Gmail, le mode d'authentification, l'intégration aux API de l'annuaire Gmail et les paramètres du proxy SEG.

4 Associez un profil EAS de modèle au déploiement MEM, puis cliquez sur **Suivant**.

   a Créez un profil EAS de modèle pour ce déploiement.

   Les nouveaux profils de modèle ne sont pas automatiquement publiés sur les terminaux. Vous pouvez publier les profils sur vos terminaux depuis la page des profils.

   b (Facultatif) Associez un profil existant à ce déploiement si plusieurs déploiements MEM doivent être configurés dans un même groupe organisationnel.

   La page de **résumé de la configuration MEM** affiche les détails de la configuration.

5 **Enregistrez** les paramètres.

6 Une fois enregistrés, vous pouvez ajouter des paramètres avancés à ce déploiement.

   a Cliquez sur l'icône **Avancé**  correspondant à votre déploiement.

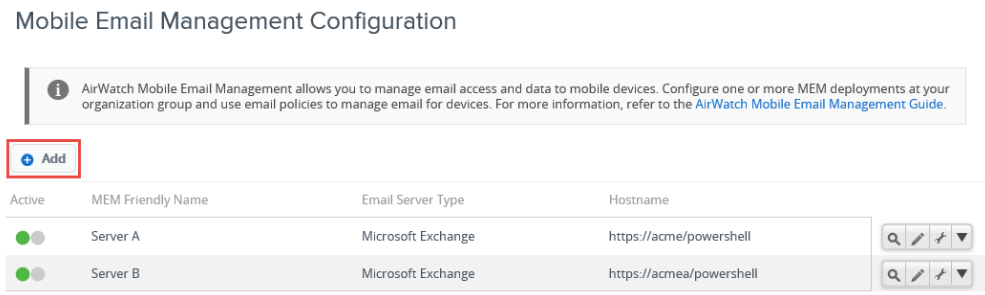
   b Configurez les paramètres disponibles pour les boîtes aux lettres des utilisateurs comme faisant partie des conditions requises sur la page **Configuration avancée de la gestion de la messagerie mobile**.

   c Cliquez sur **Enregistrer**.

Étapes suivantes

Pour configurer plusieurs déploiements MEM, sélectionnez **Ajouter** (disponible sur la page principale **Configuration de la gestion de la messagerie mobile**) et suivez les étapes 2 à 7.

Pour un déploiement SEG, vous pouvez attribuer une configuration particulière par défaut à l'aide de l'option **Définir par défaut** disponible sous  .



Note

- Vous devez créer des groupes d'utilisateurs lors de la connexion de plusieurs environnements PowerShell au même serveur Exchange.
- Utilisez différents domaines dans la configuration lors de la connexion aux différents environnements Gmail.
- Envisagez la connexion à SEG et l'intégration PowerShell au même environnement de messagerie uniquement au cours de la migration des déploiements MEM avec les paramètres appropriés. Le support Workspace ONE peut vous aider avec cette implémentation.

Activer la messagerie basée sur les certificats

L'utilisation des certificats plutôt que des identifiants habituels (nom d'utilisateur et mot de passe) présente certains avantages, notamment une authentification plus forte contre les accès non autorisés. Cela permet également de supprimer l'obligation pour les utilisateurs finaux de saisir un mot de passe ou de le renouveler tous les mois. Les e-mails sensibles entre les destinataires peuvent être chiffrés à travers le S/MIME. Vous pouvez également prouver votre identité grâce à la signature du message.

1 Naviguez vers **Terminaux > Profils et ressources > Profils**.

2 Sélectionnez**Ajouter > Ajouter un profil** puis choisissez la plateforme requise.

3 Choisissez le paramètre de profil **Identifiants** et configurez-le.

   a Pour **Source des identifiants**, choisissez parmi les éléments disponibles dans la liste.

   Les choix sont les suivants :

   - **Importer** – Importez un certificat et saisissez un nom pour celui-ci.
   - **Autorité de certification définie** – Sélectionnez la CA et le modèle de certificat à partir du menu déroulant disponible pour votre groupe organisationnel.

     Les autorités de certification et les modèles sont ajoutés pour un groupe organisationnel dans **Terminaux > Certificats > Autorités de certification**.

4 **Enregistrez et publiez** les paramètres.

Configuration de l'attribut de l'utilisateur pour les appels MEM à la suite de produits Google

Par défaut, les déploiements Gmail utilisent les API Google pour gérer l'accès à Gmail. Vous pouvez identifier l'utilisateur de l'inscription avec l'adresse e-mail de l'utilisateur lors de l'envoi de commandes à Google. Sinon, un administrateur peut également sélectionner un attribut personnalisé Active Directory au lieu de l'adresse e-mail de l'utilisateur pour identifier l'utilisateur dans Google.

Cet attribut personnalisé peut être utilisé lorsque l'adresse e-mail Google se trouve dans un champ d'attribut personnalisé de l'Active Directory du client. Les paramètres d'attribut personnalisé s'appliquent aux Google Apps utilisant le provisionnement du mot de passe, aux Google Apps avec les API directes et SEG V2 avec des méthodes de déploiement de provisionnement du mot de passe automatique.

1 Accédez à **Comptes > Administrateurs > Paramètres d'administrateur > Services d'annuaire > Utilisateur**. L'administrateur Workspace ONE UEM peut mapper les valeurs d'attributs personnalisés et utiliser la valeur de mappage de l'annuaire Active Directory des clients.

2 Activez l'attribut personnalisé sur la page **Services d'annuaire**, entrez une valeur de mappage et synchronisez les utilisateurs Active Directory pour mettre à jour l'attribut personnalisé de l'utilisateur d'inscription. Pour plus d'informations sur l'activation de l'attribut personnalisé, reportez-vous à la section Mappage des informations sur l'utilisateur des services d'annuaire du guide Intégration des services d'annuaire.

3 Accédez à **E-mail > Paramètres des e-mails** et cliquez sur **Configurer**. Configurez la passerelle de la plateforme et sélectionnez **Suivant**.

4 Sur la page **Ajouter une configuration de messagerie**, sélectionnez le modèle de déploiement **Direct**, le type d'e-mail **Google Apps avec l'API direct** et sélectionnez **Suivant**.

5 Entrez un nom convivial pour ce déploiement sur la page Déploiement. Saisissez les détails des paramètres Gmail, le mode d'authentification, l'intégration aux API de l'annuaire Gmail et les paramètres du proxy SEG.

6 Saisissez **Adresse e-mail de l'utilisateur Google**. La valeur par défaut d'Adresse e-mail de l'utilisateur Google est Adresse e-mail. Un administrateur peut sélectionner un attribut personnalisé au lieu de l'adresse e-mail par défaut.

7 Configurez les profils de messagerie. Voir Chapitre 6 Configuration des profils de messagerie .

Résultat :

Vous pouvez utiliser l'attribut personnalisé lorsque l'adresse e-mail Google se trouve dans un champ d'attribut personnalisé de l'Active Directory du client.

Attribution des terminaux dans Mobile Email Management

5

L'enregistrement des terminaux, l'attribution des profils de messagerie aux terminaux et la modification du statut de conformité des terminaux ont un impact sur MEM. Les configurations MEM sont attribuées aux terminaux en fonction des profils EAS figurant dans ces terminaux. Les politiques de conformité Géré et Profil ActiveSync requis garantissent que les configurations manuelles et non gérées ne sont pas autorisées.

Terminaux disposant d'un profil Exchange Active Sync (EAS)

Lorsqu'un terminal avec profil EAS est associé à une configuration MEM particulière, Workspace ONE UEM envoie les mises à jour de la politique à cette configuration MEM. Cette fonctionnalité facilite les migrations et permet d'utiliser plusieurs configurations MEM lors de la gestion d'un ou de plusieurs environnements de messagerie.

Quel que soit le client de messagerie, tous les modèles MEM Google nécessitent un profil EAS. Pour les nouvelles installations, l'association d'un profil EAS à une configuration MEM est obligatoire. Pour les mises à niveau, un administrateur doit associer un profil EAS à la configuration MEM une fois le processus de mise à niveau terminé.

Proxy SEG intégré

Workspace ONE UEM envoie un message de diffusion à toutes les configurations MEM du groupe organisationnel dans lequel le terminal est enrôlé. Ce message indique le statut de conformité du terminal. Lorsque la conformité change, un message signalant la mise à jour est envoyé. Lorsque le terminal se connecte à un serveur SEG particulier, le SEG reconnaît le terminal à partir du message de diffusion envoyé précédemment. Le proxy SEG signale à VMware AirWatch le terminal comme détecté. Workspace ONE UEM associe ensuite le terminal à la configuration MEM pour SEG et l'affiche sur le tableau de bord des e-mails.

Si plusieurs serveurs SEG sont soumis à l'équilibrage de charge, les messages de diffusion d'une stratégie unique s'appliquent seulement à une passerelle SEG. Cela comprend les messages envoyés depuis Workspace ONE UEM Console vers SEG lors de l'enrôlement, ou en cas de correction ou de violation de la conformité. Utilisez DeltaSync avec un intervalle de réactualisation de dix minutes pour aider les terminaux nouvellement enrôlés ou conformes. Ces terminaux connaissent une attente de dix minutes maximum avant la synchronisation de la messagerie.

Avantages :

- Des stratégies mises à jour depuis la même source d'API pour tous les serveurs SEG ;
- Un impact moindre sur les performances du serveur d'API ;
- Une complexité d'installation et de maintenance réduite comparée au modèle clustering SEG ;
- Des points d'échec moins nombreux, SEG étant responsable de ses propres stratégies ;
- Une meilleure expérience utilisateur.

PowerShell intégré

Les configurations PowerShell MEM se comportent de la même manière que les SEG en termes de mises à jour des stratégies. Pour les migrations vers PowerShell, il est important d'associer de nouveaux profils à la configuration PowerShell MEM. L'association d'un nouveau profil réduit les communications inutiles avec l'ancienne configuration MEM.

Gmail intégré

Des profils sont nécessaires pour ce type de déploiement, sauf lors de l'intégration avec les API de Google Directory. À moins que les terminaux ne soient configurés avec les profils, ils ne sont pas identifiés ni gérés par le déploiement Gmail configuré.

Synchroniser des terminaux

Utilisez MEM pour synchroniser les terminaux associés à un groupe organisationnel.

Une fois le déploiement Mobile Email Management (MEM) configuré, les terminaux du groupe organisationnel associé se synchronisent avec MEM. Vous pouvez consulter l'état des terminaux et d'autres détails sur la page **Tableau de bord des e-mails** de Workspace ONE UEM Console.

L'affichage des terminaux sur le tableau de bord dépend des modèles de déploiement auxquels les terminaux sont attribués.

- Proxy SEG – Les terminaux gérés par le proxy SEG s'affichent dans le tableau de bord lorsque le proxy SEG signale le terminal comme connecté et géré.
- Les terminaux gérés avec PowerShell s'affichent sur le tableau de bord lorsque Workspace ONE UEM envoie l'applet de commande PowerShell, autorisant le terminal à se connecter à la messagerie.
- Gmail – Les terminaux gérés avec Gmail s'affichent dans le tableau de bord lorsque le profil EAS de Workspace ONE UEM pour le proxy SEG est dans la file d'attente pour le terminal.

Le tableau de bord des e-mails indique l'un des statuts suivants :

- **Terminaux attribués** – Terminaux enrôlés avec un identifiant de configuration MEM (*memconfigID*) reconnu.
- **Terminaux non attribués** – Terminaux enrôlés pour lesquels l'identifiant de configuration MEM (*memConfigID*) n'a pas encore été identifié à travers l'attribution de profil ou la détection automatique.

- **Terminaux non gérés non détectés** – Terminaux qui ne sont pas encore enrôlés dans Workspace ONE UEM et en attente de détection automatique au niveau du groupe organisationnel par une configuration MEM.

Configuration des profils de messagerie

6

Pour déployer une messagerie EAS à l'aide du client Gmail (Android), créez un profil de configuration pour le client Gmail.

1 Naviguez vers **Terminaux > Profils et ressources > Profils > Ajouter > Ajouter un profil > Android**.

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

3 Configurez les paramètres du profil de l'onglet **Général**. Ces paramètres déterminent la façon dont le profil est déployé et les utilisateurs qui le reçoivent.

4 Sélectionnez la section de configuration **Exchange ActiveSync**.

5 Configurez les paramètres **Exchange ActiveSync**.

Paramètre	Description
Client de messagerie	Sélectionnez **Gmail** comme type de client de messagerie.
Nom du compte	Saisissez une description du compte de messagerie.
Hôte Exchange ActiveSync	Saisissez l'URL externe du serveur ActiveSync de votre entreprise. Le serveur ActiveSync peut être n'importe quel serveur de messagerie utilisant le protocole ActiveSync, comme HCL Notes Traveler, Novell Data Synchronizer et Microsoft Exchange. Dans le cas des déploiements Secure Email Gateway (SEG), utilisez l'URL de la SEG et non l'URL du serveur de messagerie.
Ignorer les erreurs SSL	Activez la fonction Ignorer les erreurs SSL pour les processus Workspace ONE Intelligent Hub.
Domaine	Saisissez le domaine de l'utilisateur final. Vous pouvez utiliser les valeurs de recherche au lieu de créer des profils individuels pour chaque utilisateur.
Utilisateur	Saisissez le nom de l'utilisateur final. Vous pouvez utiliser les valeurs de recherche au lieu de créer des profils individuels pour chaque utilisateur.

Paramètre	Description
Adresse e-mail	Saisissez l'adresse e-mail de l'utilisateur final. Vous pouvez utiliser les valeurs de recherche au lieu de créer des profils individuels pour chaque utilisateur. **Note** Si vous utilisez l'attribut personnalisé pour GSuite, vous devez utiliser la valeur de recherche d'attribut personnalisé pour le champ **Adresse e-mail** sur le profil d'e-mail Exchange ActiveSync. Consultez la page Configuration de l'attribut de l'utilisateur pour les appels MEM sur les produits Google Suite.
Mot de passe	Saisissez le mot de passe de l'utilisateur final. Vous pouvez utiliser les valeurs de recherche au lieu de créer des profils individuels pour chaque utilisateur.
Certificat d'identité	Dans le menu déroulant, sélectionnez (le cas échéant) un certificat d'identité si vous exigez que l'utilisateur final valide un certificat pour se connecter à Exchange ActiveSync. Sinon, cliquez sur **Aucun** (par défaut). Pour plus d'informations sur la sélection d'un certificat pour cette charge utile, reportez-vous au profil Déploiement des identifiants.
Synchronisation des e-mails depuis	Sélectionnez depuis combien de jours les e-mails devraient se synchroniser avec le terminal.
Synchronisation du calendrier depuis	Sélectionnez depuis combien de jours le calendrier devrait se synchroniser avec le terminal.
Synchroniser le calendrier	Autorisez le calendrier à se synchroniser avec le terminal.
Synchroniser les contacts	Autorisez les contacts à se synchroniser avec le terminal.
Autoriser la synchronisation des tâches	Autorisez les tâches à se synchroniser avec le terminal.
Taille maximum de troncature d'e-mail	Précisez la taille au-delà de laquelle les e-mails sont tronqués lorsqu'ils se synchronisent avec le terminal.
Signature d'e-mail	Saisissez la signature d'e-mail à afficher dans le courrier sortant.
Autoriser les pièces jointes	Autorisez les pièces jointes aux e-mails.
Taille maximale des pièces jointes	Définissez la taille maximum des pièces jointes en Mo.
Autoriser le transfert d'e-mails	Autorisez le transfert d'e-mails.
Autoriser le format HTML	Précisez si l'e-mail synchronisé avec le terminal peut être au format HTML. Si ce format n'est pas accepté, tous les e-mails sont convertis en texte brut.
Désactiver les captures d'écran	Désactivez les captures d'écran sur le terminal.
Intervalle de synchronisation	Saisissez le nombre de minutes entre chaque synchronisation.

Paramètre	Description
Jours de pointe pour la synchronisation du calendrier	■ Planifiez les jours de pointe pour la synchronisation, ainsi que l'**heure de début** et l'**heure de fin** de la synchronisation les jours sélectionnés. ■ Définissez la fréquence pour **Synchroniser le calendrier en heures de pointe** et**Synchroniser le calendrier en heures creuses**. ■ Le mode **automatique** synchronise la messagerie à chaque mise à jour. ■ Le mode **manuel** synchronise la messagerie uniquement à la demande. ■ L'indication d'une valeur de temps permet de synchroniser la messagerie selon un calendrier défini. ■ Activez les fonctions **Utiliser le SSL**, **Utiliser TLS** et **Compte par défaut**, le cas échéant.
Paramètres S/MIME	Cliquez sur **Utiliser S/MIME**, puis sélectionnez un certificat S/MIME comme **Certificat utilisateur** dans la section de configuration **Identifiants**. ■ **Certificat S/MIME** – Sélectionnez le certificat à utiliser. ■ **Exiger le chiffrement des messages S/MIME** – Activez cette option pour exiger le chiffrement. ■ **Exiger des messages S/MIME signés** – Activez cette option pour exiger des messages S/MIMEsignés. Indiquez un **hôte de migration** si vous utilisez des certificats S/MIME pour le chiffrement. Cliquez sur **Enregistrer** pour sauvegarder le paramètre ou **Enregistrer et publier** pour sauvegarder et appliquer les paramètres du profil au terminal concerné.

6 Cliquez sur **Enregistrer** pour sauvegarder le paramètre ou **Enregistrer et publier** pour sauvegarder et appliquer les paramètres du profil au terminal concerné.

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

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

1 Naviguez vers **Terminaux > Profils et ressources > Profils > Ajouter.** Sélectionnez **Apple iOS**.

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

3 Sélectionnez la section de configuration **Exchange ActiveSync**.

4 Sélectionnez **Client de messagerie natif** en tant que **Client de messagerie**. Complétez la zone de texte **Nom du compte** avec la description de ce compte de messagerie. Remplissez le champ **Hôte Exchange ActiveSync** avec l'URL externe du serveur ActiveSync de votre entreprise.

Note Le serveur ActiveSync peut être n'importe quel serveur de messagerie utilisant le protocole ActiveSync, comme HCL Notes Traveler, Novell Data Synchronizer et Microsoft Exchange. Dans le cas des déploiements Secure Email Gateway (SEG), utilisez l'URL de la SEG et non l'URL du serveur de messagerie.

5 Cochez la case **Utiliser SSL** afin d'activer l'utilisation de SSL (Secure Socket Layer) pour le trafic de messagerie entrant.

6 Cochez la case **S/MIME** pour utiliser d'autres certificats de chiffrement. Avant d'activer cette option, vérifiez que vous avez importé les certificats nécessaires dans les paramètres de profil **Identifiants**.

   a Sélectionnez le **certificat S/MIME** pour signer les messages des e-mails.

   b Sélectionnez le **certificat de chiffrement S/MIME** pour signer et chiffrer les messages des e-mails.

   c Activez l'option **Par message** pour permettre aux utilisateurs de choisir les messages qu'ils souhaitent signer et chiffrer en utilisant le client de messagerie natif iOS (iOS 8 et versions ultérieures supervisées uniquement).

7 Remplissez les **Informations de connexion** (**Nom de domaine, Nom d'utilisateur et Adresse e-mail**) à l'aide des valeurs de recherche. Les valeurs de recherche viennent directement de l'enregistrement du compte utilisateur. Pour utiliser les valeurs de recherche {EmailUserName} et {EmailDomain}, assurez-vous que les comptes utilisateur Workspace ONE UEM disposent d'une adresse e-mail et d'un nom d'utilisateur de messagerie définis.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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.

1 Accédez à **Terminaux > Profils > Affichage en liste > Ajouter** et cliquez sur **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 :

Paramètre	Description
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.

Paramètre	Description
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.

Application du contrôle d'accès à la messagerie 7

Configurez le contrôle d'accès pour fournir un accès sécurisé à votre infrastructure de messagerie.

Politiques de conformité des e-mails

Une fois la messagerie déployée, vous pouvez protéger davantage vos e-mails en ajoutant le contrôle d'accès. Cette fonctionnalité autorise uniquement les terminaux protégés et conformes à accéder à votre infrastructure de messagerie. Le contrôle d'accès est appliqué avec l'aide des politiques de conformité.

Ces dernières améliorent la sécurité en limitant l'accès à la messagerie pour les terminaux non gérés, inactifs, non chiffrés ou non conformes. Ces politiques vous autorisent à donner accès à la messagerie uniquement pour les terminaux approuvés et obligatoires. Elles limitent également l'accès aux e-mails en fonction du modèle de terminal et des systèmes d'exploitation.

Les catégories de ces politiques sont les suivantes : politiques générales des e-mails, politiques des terminaux gérés et politiques de sécurité des e-mails. Les différentes politiques correspondant à chaque catégorie et les déploiements auxquels elles s'appliquent sont listés dans le tableau :

Le tableau suivant répertorie les stratégies de conformité des e-mails prises en charge.

Tableau 7-1. Politiques de conformité des e-mails prises en charge

	SEG (Exchange, HCL Traveler, G suite)	PowerShell (Exchange)	Gestion des mots de passe (Gmail)	Intégration directe (Gmail)
Stratégies générales des e-mails				
Paramètres de synchronisation	O	N		
Terminal géré	O	O		
Client de messagerie	O	O		
Utilisateur	O	O		
Type de terminal EAS	O	O		
Politiques de terminaux gérés				

Tableau 7-1. Politiques de conformité des e-mails prises en charge (suite)

	SEG (Exchange, HCL Traveler, G suite)	PowerShell (Exchange)	Gestion des mots de passe (Gmail)	Intégration directe (Gmail)
Inactivité	O	O		
Terminal compromis	O	O		
Chiffrement	O	O		
Modèle	O	O		
Système d'exploitation	O	O		
Profil ActiveSync requis	O	O		
Politiques de sécurité des e-mails				
Classification de la sécurité des e-mails	O	N		
Pièces jointes (terminaux gérés)	O	N		
Pièces jointes (terminaux non gérés)	O	N		
Lien hypertexte	O	N		

Activer une politique de conformité des e-mails

Les stratégies de conformité des e-mails disponibles dans Workspace ONE UEM Console sont les politiques générales des e-mails, la politique des terminaux gérés et la politique de sécurité des e-mails. Vous pouvez activer chacune de ces politiques de conformité ou en modifier les règles afin d'autoriser ou bloquer les terminaux.

1 Accédez à **E-mail > Stratégies de conformité**.

2 Utilisez l'icône Modifier la politique sous la colonne **Actions** pour modifier n'importe quelle règle de politique.

Note Les **Politiques générales des e-mails** appliquent les politiques d'accès à la messagerie pour tous les terminaux. En choisissant un groupe d'utilisateurs, la politique s'applique à tous les utilisateurs de ce groupe.

Politique de messagerie	Description
Paramètres de synchronisation	Empêche la synchronisation des terminaux avec des fichiers EAS spécifiques. ■ Workspace ONE UEM empêche les terminaux de se synchroniser avec les dossiers sélectionnés quelles que soient les autres stratégies de conformité. ■ Pour que cette politique soit effective, le profil EAS doit être republié sur les terminaux, ce qui contraint ces derniers à se resynchroniser au serveur de messagerie.
Terminal géré	Limite l'accès aux e-mails pour les terminaux gérés uniquement.
Client de messagerie	Limite l'accès aux e-mails pour un ensemble de clients de messagerie. ■ Vous pouvez autoriser ou non les clients de messagerie selon le type de client, tel que **personnalisé** et **détecté**. ■ Vous pouvez également définir des actions par défaut pour le client de messagerie et des clients de messagerie nouvellement découverts qui n'apparaissent pas dans le champ Client de messagerie. Pour le type de client personnalisé, les caractères génériques (*) et le remplissage automatique sont pris en charge.

Politique de messagerie	Description
Utilisateur	Limite l'accès aux e-mails pour un ensemble d'utilisateurs. Vous pouvez autoriser ou non le type d'utilisateur suivant : Personnalisé, Détecté, Compte utilisateur et Groupe d'utilisateurs Workspace ONE UEM. Vous pouvez également définir des actions par défaut pour les noms d'utilisateur de messagerie qui ne s'affichent pas dans le menu déroulant Groupe ou Nom d'utilisateur. Pour le type d'utilisateur personnalisé, les caractères génériques (*) et le remplissage automatique sont pris en charge.
Type de terminal EAS	Autorise ou bloque les terminaux selon l'attribut du type de terminal EAS signalé par le terminal. Vous pouvez autoriser ou non les terminaux selon le type de client, tel que le client de messagerie personnalisé ou détecté. Vous pouvez également définir des actions par défaut pour les types de terminaux EAS qui n'apparaissent pas dans le menu déroulant Type de terminal. Pour le type de client personnalisé, les caractères génériques (*) et le remplissage automatique sont pris en charge.

Les **Politiques des terminaux gérés** appliquent les politiques aux terminaux gérés accédant à la messagerie.

Politique de messagerie	Description
Inactivité	Empêchez les terminaux gérés inactifs d'accéder aux e-mails. Vous pouvez indiquer le nombre de jours durant lesquels un terminal apparaît comme inactif (c'est-à-dire qu'il n'effectue pas de check-in dans VMware AirWatch) avant que Workspace ONE UEM n'empêche l'accès à la messagerie. La valeur minimum acceptée est 1 et la valeur maximum est 32767.
Terminal compromis	Empêchez les terminaux compromis d'accéder à la messagerie. Cette politique ne bloque pas l'accès à la messagerie pour les terminaux dont le statut « compromis » n'a pas été rapporté à AirWatch.
Chiffrement	Empêchez l'accès aux e-mails pour les terminaux non chiffrés. Cette politique s'applique seulement aux terminaux dont le statut de protection des données a été rapporté à VMware AirWatch.
Modèle	Limitez l'accès à la messagerie en fonction de la plateforme et du modèle de terminal.

Politique de messagerie	Description
Système d'exploitation	Limitez l'accès à la messagerie pour un ensemble de systèmes d'exploitation sur des plateformes spécifiques.
Profil ActiveSync requis	Empêchez l'accès à la messagerie pour les terminaux qui ne sont pas gérés avec un profil Exchange ActiveSync. Pour les clients de messagerie configurés par l'intermédiaire d'une configuration d'application plutôt qu'un profil ActiveSync, l'envoi d'une configuration d'application à un client de messagerie géré garantit que le client de messagerie est conforme à la stratégie de conformité.

Les **Politiques de sécurité de la messagerie** appliquent les politiques aux pièces jointes et aux liens hypertextes. Cette stratégie s'applique aux déploiements SEG uniquement. Pour plus d'informations, reportez-vous à la section *Application du contrôle d'accès à la messagerie*.

Politique de messagerie	Description
Classification de la sécurité des e-mails	Définissez la stratégie à appliquer par SEG pour les e-mails avec et sans étiquettes. Vous pouvez utiliser les étiquettes prédéfinies ou en créer à l'aide de l'option Personnalisé. En fonction de la classification, vous pouvez choisir d'autoriser ou de bloquer les e-mails dans des clients de messagerie.
Pièces jointes (terminaux gérés)	Chiffrez les pièces jointes des types de fichiers sélectionnés. Ces pièces jointes sont protégées sur le terminal et ne sont disponibles qu'à l'affichage dans VMware AirWatch Content Locker. Actuellement, cette fonctionnalité n'est disponible que pour les périphériques Android et iOS gérés disposant de l'application VMware AirWatch Content Locker. Pour les autres terminaux gérés, vous pouvez choisir d'autoriser les pièces jointes chiffrées, de bloquer les pièces jointes ou d'autoriser les pièces jointes non chiffrées.

Politique de messagerie	Description
Pièces jointes (terminaux non gérés)	Chiffrez et bloquez les pièces jointes ou autorisez les pièces jointes non chiffrées pour les terminaux non gérés. Les pièces jointes chiffrées ne sont pas visibles sur les terminaux non gérés. Cette fonctionnalité vise à préserver l'intégrité de la messagerie. Si un e-mail contenant une pièce jointe chiffrée est transféré depuis un terminal non géré, le destinataire peut toujours l'afficher sur un PC ou un autre terminal mobile.
Lien hypertexte	Autorisez l'ouverture de liens hypertexte contenus dans un e-mail directement depuis VMware Browser installé sur le terminal. Secure Email Gateway modifie dynamiquement le lien hypertexte à ouvrir dans VMware Browser. Vous pouvez choisir l'un des types de modification suivant : ■ Tous/Toutes - Choisissez d'ouvrir tous les liens hypertexte avec VMware Browser. ■ Exclure - Précisez si vous ne souhaitez pas que les utilisateurs ouvrent les domaines mentionnés via VMware Browser. Indiquez les domaines exclus dans le champ **Modifier tous les liens hypertexte sauf pour ces domaines**. Vous pouvez également importer par lot les noms de domaine depuis un fichier `.csv`. ■ Inclure - Décidez si vous souhaitez que l'utilisateur ouvre les liens hypertexte depuis des domaines spécifiés via VMware Browser. Indiquez les domaines exclus dans le champ **Modifier seulement les liens hypertexte pour ces domaines**. Vous pouvez également importer par lot les noms de domaine depuis un fichier `.csv`.

3 Créez votre règle de conformité et **enregistrez**-la.

4 Sélectionnez le bouton gris sous la colonne **Actif** pour activer la politique de conformité. Une page s'affiche avec un code.

5 Saisissez le code dans le champ correspondant, puis sélectionnez **Continuer**.

Résultat : la politique est activée, ce qui est signalé par un cercle vert dans la colonne **Actif**.

Protection du contenu des e-mails, des pièces jointes et des liens hypertexte

Sécurisez vos e-mails avec Workspace ONE UEM Web et Workspace ONE UEM Content.

Workspace ONE UEM vous aide à protéger et à contrôler les pièces jointes sensibles à la perte des données pour les terminaux gérés et non gérés. Workspace ONE UEM autorise l'ouverture de liens hypertexte contenus dans un e-mail directement depuis Workspace ONE Web installé sur le terminal. Secure Email Gateway modifie dynamiquement le lien hypertexte à ouvrir dans Workspace ONE Web.

Vous devez avoir installé les applications suivantes avant de pouvoir commencer à protéger vos pièces jointes :

- Secure Email Gateway (SEG)
- VMware Content Locker (iOS et Android)
- Prise en charge de Microsoft Exchange 2010/2013/2016/2019, HCL Notes, Novell GroupWise et Gmail

Activer la classification de la sécurité des e-mails

Sélectionnez les classifications de sécurité sur la console UEM Workspace ONE UEM Console pour laquelle vous souhaitez que Secure Email Gateway prenne des mesures.

Il existe une liste de classifications de la sécurité prédéfinies. Vous pouvez également créer votre classification personnalisée.

1 Accédez à **E-mail > Stratégies de conformité > Stratégies de sécurité des e-mails**.

2 Sélectionnez le cercle gris sous la colonne **Actif** pour la politique de conformité **Classification de la sécurité des e-mails**. Une page s'affiche avec un code.

3 Saisissez le code dans le champ correspondant, puis sélectionnez **Continuer**. La politique est activée, ce qui est signalé par un cercle vert dans la colonne **Actif**.

4 Sélectionnez l'option **Modifier** sous la colonne **Actions**.

5 Sélectionnez **Ajouter**, puis le type d'étiquette dans le menu déroulant **Type**.

   Les options disponibles sont « Prédéfini » et « Personnalisé ». Les choix sont les suivants :

   - Sélectionnez le type d'étiquette « Prédéfini » pour obtenir une liste d'étiquettes disponibles dans le menu déroulant **Classification de la sécurité**.
   - Sélectionnez le type d'étiquette « Personnalisé » pour saisir votre propre étiquette dans le champ **Classification de la sécurité**.

6 Saisissez une **description** de l'étiquette, puis cliquez sur **Suivant**.

7 Configurez les actions à mener par SEG à l'encontre des e-mails marqués ou non d'une étiquette. Sélectionnez **Suivant**.

   Vous pouvez choisir d'autoriser ou de bloquer les e-mails dans des clients de messagerie.

8 Affichez le **résumé**, puis cliquez sur **Enregistrer**.

Protection des pièces jointes aux e-mails

Protégez les pièces jointes à l'aide de Workspace ONE UEM.

Les pièces jointes correspondent à différents types de fichiers. Dans UEM Console, vous pouvez sélectionner les types de fichiers pour lesquels les pièces jointes doivent être chiffrées par Secure Email Gateway. Ces pièces jointes chiffrées sont protégées sur les terminaux mobiles et peuvent être consultées dans l'application VMware AirWatch Content Locker.

Les paramètres granulaires sont disponibles pour les périphériques Android et iOS gérés. Pour les autres terminaux gérés et tous les terminaux non gérés, l'ouverture (en masse) des pièces jointes peut être empêchée dans les applications tierces.

1 Accédez à **E-mail > Stratégies de conformité > Stratégies de sécurité des e-mails**.

2 Sélectionnez le bouton gris sous la colonne **Actif** pour la stratégie de conformité des **pièces jointes (terminaux gérés)** ou des **pièces jointes (terminaux non gérés)**.

   Résultat : une page s'affiche avec un code.

3 Saisissez le code dans le champ correspondant, puis sélectionnez **Continuer**.

   Résultat : la politique est activée, ce qui est signalé par un cercle vert dans la colonne **Actif**.

4 Sélectionnez l'option **Modifier** sous la colonne **Actions**.

5 Choisissez de chiffrer et autoriser ou de bloquer ou autoriser, sans chiffrer les pièces jointes, pour chaque catégorie de fichiers (périphériques Android et iOS gérés uniquement).

6 Cochez la case **Autoriser l'enregistrement des pièces jointes dans le Content Locker** pour enregistrer les pièces jointes dans le Content Locker.

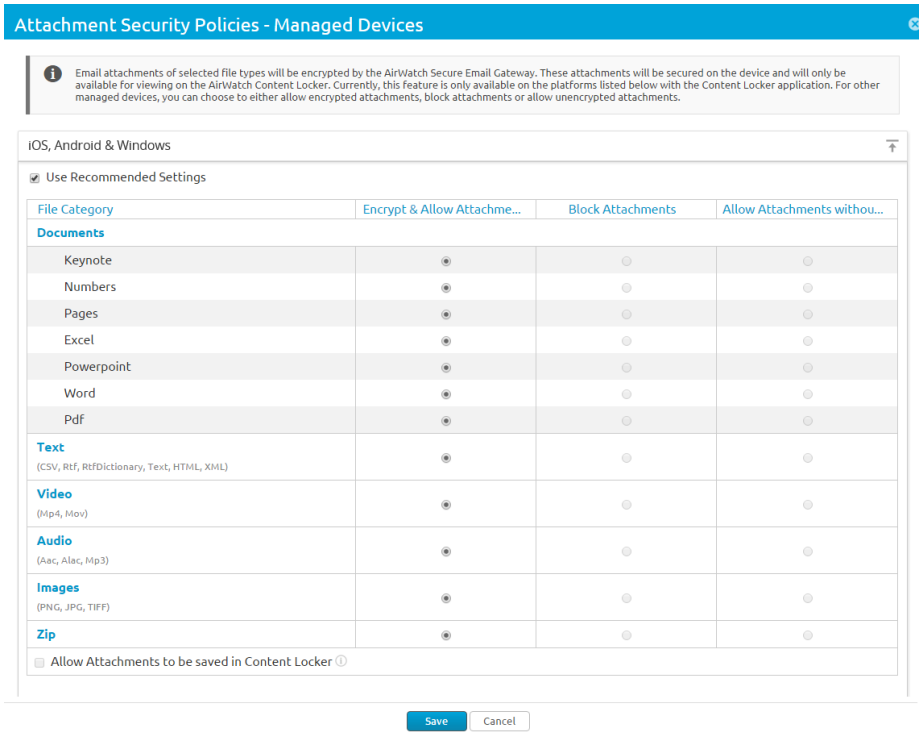
   Résultat : les pièces jointes restent chiffrées et les politiques du Content Locker s'appliquent.

7 Choisissez la politique pour tous les **autres fichiers** non mentionnés ici.

8 Saisissez les extensions de fichier qui doivent être exclues des actions configurées dans les **autres fichiers**, dans la **liste d'exclusions**.

9 Saisissez un **Message personnalisé pour les pièces jointes bloquées** afin d'informer le destinataire qu'une pièce jointe a été bloquée.

10 **Enregistrez** les paramètres.



Activer la protection des liens hypertexte

Avec la politique de sécurité des liens hypertexte, vous pouvez contrôler les liens hypertexte à modifier afin qu'ils puissent être ouverts directement dans Workspace ONE Web.

1 Accédez à **E-mail > Stratégies de conformité > Stratégies de sécurité des e-mails**.

2 Sélectionnez le cercle gris sous la colonne **Actif** pour la politique de conformité des **liens hypertexte**.

Résultat : une page s'affiche avec un code.

3 Saisissez le code dans le champ correspondant, puis sélectionnez **Continuer**.

Résultat : la politique est activée, ce qui est signalé par un cercle vert dans la colonne **Actif**.

4 Sélectionnez l'option **Modifier** sous la colonne **Actions**.

5 Sélectionnez la plate-forme pour laquelle vous souhaitez ignorer la transformation des liens hypertexte.

6 Sélectionnez l'un des **Types de modification**

Les choix sont les suivants :

- **Tous/Toutes** – Choisissez d'ouvrir tous les liens hypertexte avec Workspace ONE Web.
- **Inclure** – Décidez si vous souhaitez que l'utilisateur ouvre les liens hypertexte depuis des domaines spécifiés via Workspace ONE Web. Indiquez les domaines exclus dans le champ **Modifier seulement les liens hypertexte pour ces domaines**. Vous pouvez également importer en masse les noms de domaine depuis un fichier .csv.

- **Exclure** - Précisez si vous ne souhaitez pas que les utilisateurs ouvrent les domaines mentionnés via Workspace ONE Web. Indiquez les domaines exclus dans la zone de texte **Modifier tous les liens hypertexte sauf pour ces domaines**. Vous pouvez également importer en masse les noms de domaine depuis un fichier .csv.

7 **Enregistrez** les paramètres.

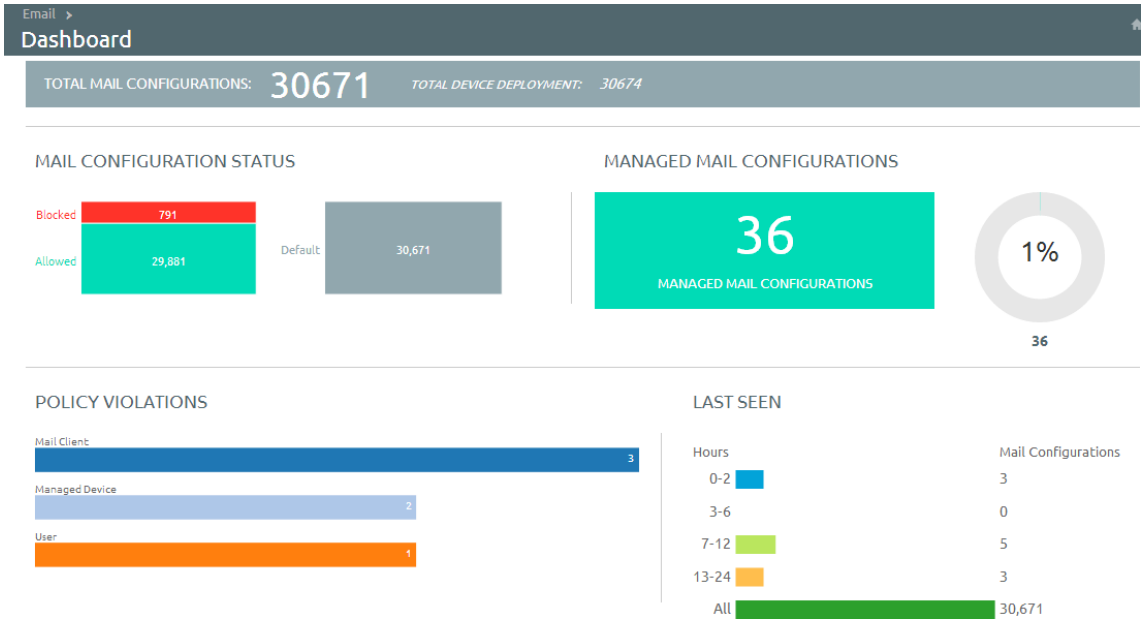
Surveiller le trafic de messagerie

8

Surveillez les terminaux et le trafic de la messagerie de vos utilisateurs grâce au **tableau de bord des e-mails**.

Le **Tableau de bord des > e-mails** offre un résumé du statut des terminaux connectés au serveur de messagerie.

Vous pouvez également utiliser les graphiques pour filtrer votre recherche. Par exemple, si vous voulez afficher tous les terminaux gérés d'un groupe organisationnel, sélectionnez le graphique Terminaux gérés. Le graphique affiche les résultats sur la page Affichage en liste.



Affichez des informations détaillées sur l'utilisateur et le terminal.

Vous pouvez afficher en temps réel toutes les mises à jour des terminaux de l'utilisateur final que vous gérez avec Mobile Email Management (MEM) sur la page **E-mail > Affichage en liste**.

Utilisez les onglets **Terminal** et **Utilisateur** pour afficher les informations relatives à chacun d'eux. Pour afficher la synthèse ou la liste personnalisée d'informations, modifiez la mise en page.

- Affichez les terminaux gérés, non gérés, conformes, non conformes, bloqués ou autorisés.

- Affichez l'adresse IP du terminal.

  Note Pour Workspace ONE UEM version 2107 et ultérieures, les détails du terminal tels que le système d'exploitation, le modèle, la plateforme, le numéro de téléphone, le numéro IMEI et autres ne s'affichent pas sur la page **Affichage en liste**.

Vous pouvez consulter les informations relatives à l'utilisateur ou à son terminal sous forme de synthèse ou de liste personnalisée en fonction de vos besoins.

La page **Affichage en liste** fournit les informations détaillées suivantes :

Paramètre	Description
Dernière demande	Dernière modification du statut du terminal effectuée depuis Workspace ONE UEM ou depuis l'intégration de PowerShell. Dans l'intégration SEG, cette colonne indique la dernière synchronisation de la messagerie au terminal.
Utilisateur	Nom du compte utilisateur.
Nom convivial	Nom convivial du terminal.
Configuration MEM	Déploiement MEM configuré qui gère le terminal.
Adresse e-mail	Adresse e-mail du compte utilisateur.
Identifiant	Code d'identification alphanumérique unique associé au terminal.
Client de messagerie	Client de messagerie synchronisant les e-mails sur le terminal.
Dernière commande	Dernière modification du statut du terminal, qui remplit automatiquement la colonne **Dernière requête**.
Dernier serveur de passerelle	Serveur auquel le terminal est connecté.

Paramètre	Description
Statut	Statut du terminal en temps réel et si la messagerie est bloquée ou non comme le veut la politique définie.
Motif	Code d'explication pour autoriser ou bloquer la messagerie sur le terminal. ■ Ce code est défini sur « Global » si les politiques par défaut de l'organisation Autoriser, Bloquer ou Mettre en quarantaine définissent le statut d'accès. Ce code est défini sur « Individuel » si l'ID du terminal est clairement défini pour une boîte aux lettres donnée par un administrateur Exchange ou Workspace ONE UEM. Ce code est défini sur « Politique » si une politique EAS bloque le terminal. ■ Workspace ONE UEM vous offre la possibilité de bloquer les e-mails sur les terminaux non conformes (tels que ceux comportant des applications sur liste bloquée). La messagerie est activée une fois les terminaux conformes. Vous pouvez afficher les terminaux non conformes sur le **tableau de bord des e-mails** marqués de l'étiquette 'Conformité MDM'.

- **Adresse IP** - Adresse IP de votre terminal.

  Note Pour Workspace ONE UEM version 2107 et ultérieures, les détails du terminal tels que le système d'exploitation, le modèle, la plateforme, le numéro de téléphone, le numéro IMEI et autres ne s'affichent pas sur la page **Affichage en liste**.

- **Identité de la boîte aux lettres** - Emplacement de la boîte aux lettres de l'utilisateur dans Active Directory.

Filtres

Réduisez la recherche en utilisant l'option **Filtre** sur la page d'affichage en liste.

Paramètres	Description
Dernière connexion	Tous/Toutes, Moins de 24 heures, Moins de 12 heures, Moins de 6 heures, Moins de 2 heures
Géré(s)	Tous, Géré(s), Non géré(s)
Autorisé	Tous, Autorisé(s), Bloqué(s)
Remplacement de la stratégie	Tous, Sur liste bloquée, Sur liste autorisée, Par défaut.
Violation de la stratégie	Terminal compromis, Terminal inactif, Données non protégées/Terminal non enrôlé/non conforme, Type de terminal/Compte de messagerie/Client de messagerie/ Modèle/OS non approuvés par EAS
Configuration MEM	Filtrez les terminaux en fonction des déploiements MEM configurés.
Type de terminal EAS	Filtrez en fonction du type de terminal.

Adresse e-mail	Filtrez en fonction de l'adresse e-mail.
Dernier serveur de passerelle	Filtrez en fonction du serveur SEG disponible.

Actions sur la messagerie

Les menus déroulants **Remplacer**, **Actions** et **Administration** offrent un seul emplacement pour effectuer plusieurs actions sur le terminal.

Important ces actions sont irréversibles.

Remplacer

Cochez la case correspondant au terminal sur lequel vous voulez effectuer une action. Mettez sur liste autorisée ou liste bloquée un terminal quelle que soit la politique de conformité, et rétablissez la politique quand cela est nécessaire.

- **Liste autorisée** : autorise le terminal à recevoir les e-mails.
- **Liste bloquée** : empêche le terminal de recevoir les e-mails.
- **Par défaut** - Autorise ou bloque un terminal selon qu'il est conforme ou non.

Actions

- **Synchroniser les boîtes aux lettres** - Envoie au serveur Exchange une demande de liste mise à jour de terminaux ayant essayé de synchroniser la messagerie (modèle direct PowerShell). Si vous ne choisissez pas cette option, la liste de terminaux non gérés ne change pas, à moins que l'un des terminaux non gérés ne soit enrôlé dans Workspace ONE UEM ou que vous mettiez manuellement sur liste autorisée ou liste bloquée un terminal, lançant alors une commande de changement d'état.

  Workspace ONE UEM offre une option de synchronisation de la messagerie au sein du portail self-service (SSP) afin que l'utilisateur final puisse synchroniser son terminal avec le serveur de messagerie et exécute également les politiques de conformité préconfigurées pour tous les terminaux. Ce processus est plus simple que la synchronisation en masse effectuée sur tous les terminaux.
- **Appliquer la conformité** - Déclenche le moteur de conformité pour la configuration MEM sélectionnée. Cette commande fonctionne différemment avec le modèle PowerShell plutôt que le modèle SEG.
  - Si le modèle SEG est configuré, cette commande met à jour les dernières politiques de conformité.
  - Si le modèle PowerShell est configuré, cette commande procède à une vérification manuelle de conformité sur tous les terminaux et bloque ou autorise l'accès du terminal à la messagerie.

Lorsque le modèle direct PowerShell est configuré, Workspace ONE UEM communique directement avec le tableau CAS en utilisant des sessions PowerShell signées à distance établies depuis le serveur de la console ou VMware Enterprise Systems Connector (selon l'architecture de déploiement). Grâce aux sessions signées à distance, les commandes PowerShell sont envoyées pour mettre sur liste bloquée et liste autorisée les ID des terminaux pour la boîte de réception CAS d'un utilisateur donné sur Exchange 2010/2013 selon l'état de conformité dans Workspace ONE UEM.

- **Activer le mode de test** - Teste les politiques de messagerie sans les appliquer aux terminaux des déploiements intégrés à SEG.

Administration

Cochez la case correspondant au terminal sur lequel vous voulez effectuer une action.

Paramètres	Description
E-mail d'enrôlement	Envoie un e-mail à l'utilisateur contenant tous les détails nécessaires à l'enrôlement. Lorsqu'un terminal non géré est détecté, envoyez un e-mail d'enrôlement demandant à l'utilisateur d'enrôler le terminal (PowerShell uniquement).
Activer le mode diagnostic	Effectue le diagnostic pour la boîte aux lettres sélectionnée et fournit l'historique des activités du terminal. Cette politique s'applique aux déploiements SEG uniquement.
Désactiver le mode diagnostic	Désactive le diagnostic pour la boîte aux lettres sélectionnée.
Mettre à jour la clé de chiffrement	Réinitialise le chiffrement, puis resynchronise les e-mails pour les terminaux sélectionnés.
Effacer à distance	Rétablit paramètres d'usine du terminal. Effectuez un effacement des données d'entreprise (réinitialisez aux paramètres d'usine) sur un terminal volé ou perdu contenant des informations sensibles (PowerShell uniquement).
Supprimer les terminaux non gérés	Supprime l'enregistrement du terminal non géré sélectionné depuis le tableau de bord.
Migrer les terminaux	Migrez les terminaux à travers les groupes organisationnels et les déploiements MEM.
Synchroniser la boîte aux lettres sélectionnée	Synchronise la boîte aux lettres du terminal sélectionné. Une seule boîte aux lettres peut être synchronisée à la fois.

Note notez que cet enregistrement peut s'afficher à nouveau après la prochaine synchronisation.

Vérification des terminaux non gérés

Pour vous assurer que tous les terminaux sont gérés et surveillés, naviguez vers la page Affichage en liste. Sur cette page, filtrez les terminaux non gérés, puis envoyez un e-mail d'enrôlement depuis le menu déroulant Administration.