# Secure Mail

## Contents



# Présentation de Secure Mail

February 19, 2019

Citrix Secure Mail permet aux utilisateurs d'accéder à leurs e-mails, calendriers et contacts sur leurs téléphones mobiles et tablettes. Pour conserver la continuité des comptes Microsoft Outlook ou IBM Notes, Secure Mail est synchronisé avec le serveur Microsoft Exchange Server et le serveur IBM Notes Traveler.

En tant qu'application Citrix, Secure Mail tire parti de la compatibilité SSO avec Citrix Secure Hub. Une fois que les utilisateurs se sont connectés à Secure Hub, ils peuvent utiliser Secure Mail sans avoir à entrer de nouveau leur nom d'utilisateur et mot de passe. Vous pouvez configurer Secure Mail afin qu'il soit automatiquement distribué sur les appareils utilisateur lorsque ces derniers sont inscrits dans Secure Hub, ou les utilisateurs peuvent ajouter l'application depuis le magasin.

Secure Mail est compatible avec :

- Exchange Server 2016, mise à jour cumulative 11
- Exchange Server 2016, mise à jour cumulative 10
- Exchange Server 2016, mise à jour cumulative 9
- Exchange Server 2016, mise à jour cumulative 8
- Exchange Server 2013, mise à jour cumulative 21
- Exchange Server 2013, mise à jour cumulative 19
- Exchange Server 2010 SP3 Update Rollup 24
- Exchange Server 2010 SP3 Update Rollup 19
- Exchange Server 2010 SP3 Update Rollup 22
- Serveur de messagerie IBM Domino version 9.0.1 FP10 HF197
- Serveur de messagerie IBM Domino version 9.0.1 FP9
- IBM Lotus Notes Traveler version 9.0.1.21
- IBM Lotus Notes Traveler version 9.0.1.9
- Microsoft Office 365 (Exchange Online)

Pour commencer, téléchargez Secure Mail et d'autres composants Endpoint Management à partir de Téléchargements de Citrix Endpoint Management.

Pour connaître la configuration système requise pour Secure Mail et pour d'autres applications de mobilité, consultez la section Configuration système requise.

Pour plus d'informations sur les notifications dans Secure Mail pour iOS et Android lorsque l'application est exécutée en arrière-plan ou fermée, consultez la section Notifications push pour Secure Mail.

Pour les fonctionnalités iOS prises en charge sur Secure Mail, voir les fonctionnalités iOS pour Secure Mail.

Pour les fonctionnalités Android prises en charge sur Secure Mail, voir les fonctionnalités Android pour Secure Mail.

Pour les fonctionnalités iOS et Android prises en charge sur Secure Mail, voir les fonctionnalités iOS et Android pour Secure Mail.

## Nouveautés dans Secure Mail

March 12, 2019

Les fonctionnalités suivantes sont nouvelles dans Secure Mail :

### Secure Mail 19.2.0

#### Secure Mail pour iOS

Secure Mail 19.2.0 inclut des améliorations de performance et des corrections de bogues.

Pour accéder aux problèmes connus et résolus, veuillez consulter Problèmes connus et résolus.

#### Secure Mail pour Android

- **Améliorations apportées aux contacts.** Dans Secure Mail pour Android, lorsque vous appuyez sur **Contacts** et sélectionnez un contact, les détails de ce contact apparaissent sous l'onglet **Contact**. Lorsque vous appuyez sur l'onglet **Organisation**, les détails de la hiérarchie de l'organisation, tels que **MANAGER**, **COLLABORATEURS DIRECTS** et **COLLÈGUES**, apparaissent. Lorsque vous appuyez sur l'icône plus en haut à droite de l'écran, les options suivantes s'affichent :
  - **Joindre au message**
  - **Partager**
  - **Supprimer**

  Dans l'onglet **Organisation**, vous pouvez appuyer sur l'icône plus située à droite de **MANAGER**, **COLLABORATEURS DIRECTS** et **COLLÈGUES** pour créer un nouvel e-mail ou une nouvelle invite de calendrier. Le champ **À :** de l'e-mail ou de l'événement de calendrier est automatiquement renseigné avec les détails de **MANAGER**, **COLLABORATEURS DIRECTS** et **COLLÈGUES**.

  **Conditions préalables :**

  Assurez-vous que Exchange Web Services (EWS) est activé sur votre serveur Exchange Server.

Les détails du contact apparaissent en fonction des détails de l'organisation extraits d'Active Directory. Pour que les détails corrects apparaissent pour vos contacts, assurez-vous que votre administrateur a configuré votre hiérarchie d'organisation dans Active Directory.

> Remarque :
>
> Cette fonctionnalité n'est pas prise en charge sur le serveur IBM Lotus Notes.

- **Stratégie d'accès réseau**. Dans Secure Mail pour Android, une nouvelle option appelée **Tunnel - SSO Web** a été ajoutée à la stratégie MDX d'accès réseau. La configuration de cette stratégie vous donne la flexibilité de tunnéliser le trafic interne via Secure Browse et Secure Ticket Authority (STA) en parallèle. Vous pouvez également autoriser les connexions Secure Browse pour les services d'authentification, tels que NTLM, Okta et Kerberos. Lorsque vous configurez initialement STA, vous devez ajouter des noms de domaine complets et des ports d'adresses de service individuels à la stratégie Services réseau d'arrière-plan. Toutefois, si vous configurez l'option **Tunnel - SSO Web**, vous n'avez pas besoin d'effectuer ces configurations.

Pour activer cette stratégie pour Secure Mail pour Android dans la console Citrix Endpoint Management :

1. Téléchargez et utilisez le fichier .mdx pour Android. Pour plus de détails, reportez-vous à la section Fonctionnement des applications mobiles et MDX.
2. Dans la stratégie d'accès réseau, cliquez sur l'option **Tunnel - SSO Web**. Pour plus d'informations, consultez Accès au réseau d'applications

## Nouveautés dans les versions précédentes

### Secure Mail pour iOS 19.1.6

Cette version inclut des améliorations de performance et des corrections de bogues.

### Secure Mail 19.1.5

À partir de cette version, Secure Mail prend en charge les serveurs suivants :

- Exchange Server 2016, mise à jour cumulative 11
- Exchange Server 2010 SP3 Update Rollup 24

Pour une liste complète de compatibilité Secure Mail-serveur, voir Présentation de Secure Mail.

### Secure Mail 19.1.0

### Secure Mail pour iOS

- **Améliorations apportées aux contacts.** Dans Secure Mail pour iOS, lorsque vous appuyez sur **Contacts** et sélectionnez un contact, les détails de ce contact apparaissent sous l'onglet **Contact**. Lorsque vous appuyez sur l'onglet **Organisation**, les détails de la hiérarchie de l'organisation, tels que **Responsable**, **Collaborateurs directs** et **Collègues**, apparaissent. Lorsque vous appuyez sur l'icône plus en haut à droite de l'écran, les options suivantes s'affichent :

  – Modifier
  – Ajouter aux VIP
  – Annul.

  Dans l'onglet **Organisation**, vous pouvez appuyer sur l'icône plus située à droite de **Responsable**, **Collaborateurs directs** ou **Collègues**. Cette action vous permet de créer un e-mail ou un événement de calendrier. Le champ **À :** de l'e-mail ou de l'événement de calendrier est automatiquement renseigné avec les détails du **responsable**, des **collaborateurs directs** ou des **collègues**. Vous pouvez composer et envoyer l'e-mail.

  **Conditions préalables :**

  Assurez-vous que Exchange Web Services (EWS) est activé sur votre serveur Exchange Server.

  Les détails du contact apparaissent en fonction des détails de l'organisation (contact Outlook) extraits d'Active Directory. Pour que les détails corrects apparaissent pour vos contacts, assurez-vous que votre administrateur a configuré votre hiérarchie d'organisation dans Active Directory.

  > Remarque :
  >
  > Cette fonctionnalité n'est pas prise en charge sur le serveur IBM Lotus Notes.

- **Exporter l'heure et le lieu de la réunion vers votre calendrier natif.** Dans Secure Mail pour iOS, une nouvelle valeur **Heure et lieu de la réunion** est ajoutée à la stratégie MDX **Exporter calendrier**. Cette amélioration vous permet d'exporter l'heure et le lieu des événements de calendrier Secure Mail vers votre calendrier natif.
- Secure Mail pour iOS prend en charge les notifications push enrichies sur les configurations exécutant Microsoft Enterprise Mobility + Security (EMS) /Intune avec authentification moderne (O365).

  Pour activer ces notifications push, assurez-vous que les conditions préalables suivantes sont remplies :

  – Dans la console Endpoint Management, activez les **notifications push**.
  – La stratégie **Accès réseau** est définie sur **Non restreint**.
  – La stratégie **Contrôler les notifications de l'écran verrouillé** est définie sur **Autoriser** ou **Expéditeur de l'e-mail ou titre de l'événement**.
  – Accédez à **Secure Mail** > **Paramètres** > **Notifications** et activez **Notifications par e-mail**.

- Les utilisateurs de Secure Mail peuvent utiliser l'application Zoom pour rejoindre des réunions. Pour plus d'informations sur la configuration des stratégies requises pour utiliser l'application Zoom, voir Rejoindre des réunions à partir du calendrier.
- Cette version inclut la prise en charge de l'iPad Pro 11 pouces et de l'iPad Pro 12,9 pouces.

#### Secure Mail pour Android

- **Amélioration des pièces jointes.** Dans Secure Mail pour Android, l'affichage des pièces jointes a été simplifié. Pour offrir une meilleure expérience, les étapes non essentielles sont supprimées, mais les options de pièces jointes qui existaient dans les versions précédentes sont conservées.

  Vous pouvez afficher les pièces jointes dans l'application Secure Mail. La pièce jointe s'ouvre directement, si elle peut être consultée à l'aide de Secure Mail ; sinon, une liste d'applications s'affiche. Vous pouvez sélectionner l'application requise pour afficher la pièce jointe. Pour plus de détails, voir Affichage des pièces jointes.
- Les utilisateurs de Secure Mail peuvent utiliser l'application Zoom pour rejoindre des réunions. Pour plus d'informations sur la configuration des stratégies requises pour utiliser l'application Zoom, voir Rejoindre des réunions à partir du calendrier.
- **Exporter l'heure et le lieu de la réunion vers votre calendrier natif.** Dans Secure Mail pour iOS, une nouvelle valeur **Heure et lieu de la réunion** est ajoutée à la stratégie MDX **Exporter calendrier**. Cela vous permet d'exporter l'heure et le lieu des événements de calendrier Secure Mail vers votre calendrier natif.

> Remarque :
>
> La prise en charge d'Android 5.x s'est terminée le 31 décembre 2018.

### Secure Mail 18.12.0

Secure Mail 18.12.0 inclut des améliorations de performance et des corrections de bogues.

Pour accéder aux problèmes connus et résolus, veuillez consulter Problèmes connus et résolus.

### Secure Mail 18.11.5

#### Secure Mail pour Android

- **Signaler des e-mails de phishing avec des en-têtes ActiveSync.** Dans Secure Mail pour Android, lorsqu'un utilisateur signale un courrier de phishing, un fichier EML est généré en tant que pièce jointe correspondant à ce courrier. Les administrateurs reçoivent ce courrier et peuvent afficher les en-têtes ActiveSync associés au courrier signalé.

Pour activer cette fonctionnalité, un administrateur doit configurer la stratégie **Signaler les adresses e-mail de phishing** et définir **Mécanisme de signalisation de phishing** sur **Signaler via pièce jointe** dans la console Citrix Endpoint Management. Pour plus de détails, consultez la section Signaler les e-mails de phishing (en tant que pièce jointe).

- **Imprimer des e-mails et des événements de calendrier.** Dans Secure Mail pour Android, vous pouvez imprimer des e-mails et des événements de calendrier à partir de votre appareil Android. Cette fonctionnalité d'impression utilise Android Print Framework. Pour plus de détails, voir Imprimer des e-mails et des événements de calendrier.
- **Flux de votre manager.** Dans Secure Mail pour Android, vous pouvez afficher les e-mails de votre manager dans l'écran **Flux**. Jusqu'à cinq e-mails apparaissent sous le flux **De votre manager**, en fonction de vos paramètres de **Période de sync. des messages**. Pour afficher plus d'e-mails de votre manager, appuyez sur **Tout afficher**.

  **Conditions préalables :**

  Assurez-vous que Exchange Web Services (EWS) est activé sur votre serveur Exchange Server.

  La carte de manager apparaît en fonction des détails de l'organisation (contact Outlook) extraits d'Active Directory. Pour que les détails corrects apparaissent dans le flux du manager, assurez-vous que votre administrateur a configuré votre hiérarchie d'organisation dans Active Directory.

  > Remarque :
  >
  > Cette fonctionnalité n'est pas prise en charge sur le serveur IBM Lotus Notes.

### Secure Mail 18.11.1

> Important :
>
> Le problème suivant est résolu dans Secure Mail pour Android 18.11.1
>
> Dans Secure Mail pour Android avec des connexions à IBM Notes Traveler 9.0.1 SP 10, les e-mails avec pièces jointes restent dans la boîte d'envoi. [CXM-58962]

### Secure Mail 18.11.0

#### Secure Mail pour Android

- **Notifications de sous-dossier.** Dans Secure Mail pour Android, vous pouvez recevoir des notifications par e-mail pour les sous-dossiers de votre compte de messagerie. Pour plus de détails, consultez la section Notifications de sous-dossier.
- **Mises à jour des services d'arrière-plan dans Secure Mail pour Android.** Pour satisfaire aux exigences de limitation d'exécution en arrière-plan de Google Play sur les appareils

fonctionnant sous Android 8.0 (API niveau 26) ou ultérieur, nous avons mis à niveau les services d'arrière-plan de Secure Mail. Pour une synchronisation et des notifications de messagerie ininterrompues sur votre appareil, activez les notifications push du service Firebase Cloud Messaging (FCM). Pour plus d'informations sur l'activation des notifications push basées sur FCM, voir Notifications push pour Secure Mail.

Assurez-vous d'activer **Notifications par e-mail** dans les paramètres de Secure Mail sur votre appareil. Pour de plus amples informations sur cette mise à jour, consultez cet article du centre de connaissances.

**Limitations :**

- Si vous n'avez pas activé les notifications push basées sur FCM, la synchronisation en arrière-plan est effectuée toutes les 15 minutes. Cet intervalle peut varier selon que l'application s'exécute en arrière-plan ou au premier plan.
- Lorsque les utilisateurs mettent à jour manuellement l'heure à partir des paramètres de l'appareil, la date du widget de calendrier ne se met pas à jour automatiquement.

**Secure Mail pour iOS**

- **Prise en charge d'iOS 12.1.** Secure Mail pour iOS prend en charge iOS version 12.1.
- **Améliorations apportées aux messages d'échec des notifications push enrichies.** Dans Secure Mail pour iOS, les messages d'échec de notification push apparaissent dans le centre de notification de votre appareil en fonction du type d'échec de notification. Pour plus d'informations sur les messages d'échec de notification Push dans Secure Mail pour iOS, voir Messages d'échec de notification push dans Secure Mail pour iOS.
- **Flux de votre manager.** Dans Secure Mail pour iOS, vous pouvez afficher les e-mails de votre manager dans l'écran **Flux**. Jusqu'à cinq e-mails apparaissent sous le flux **De votre manager**, en fonction de vos paramètres de **Période de sync. des messages**. Pour afficher plus d'e-mails de votre manager, appuyez sur **Tout afficher**.

  **Conditions préalables :**

  Assurez-vous que Exchange Web Services (EWS) est activé sur votre serveur Exchange Server.

  La carte de manager apparaît en fonction des détails de l'organisation (contact Outlook) extraits d'Active Directory. Pour que les détails corrects apparaissent dans le flux du manager, assurez-vous que votre administrateur a configuré votre hiérarchie d'organisation dans Active Directory.

  > Remarque :
  >
  > Cette fonctionnalité n'est pas prise en charge sur le serveur IBM Lotus Notes.

**Secure Mail 18.10.5**

- **Intégration de Secure Mail avec Slack (Aperçu) :** vous pouvez désormais transférer vos conversations e-mail vers l'application Slack sur les appareils fonctionnant sous iOS ou Android. Pour plus de détails, consultez la section Intégration de Secure Mail avec Slack (Aperçu).
- **Améliorations apportées au dossier Flux :** dans Secure Mail pour iOS, les améliorations suivantes sont apportées au dossier Flux existant :
  - Affichez jusqu'à cinq réunions à venir dans votre fiche Flux.
  - Les réunions à venir pour la prochaine période de 24 heures apparaissent dans la fiche Flux et sont classées dans les sections **Aujourd'hui** et **Demain**.

**Secure Mail 18.10.0**

- **Canaux de notification Secure Mail pour les notifications par e-mail et calendrier :** sur les appareils fonctionnant sous Android O ou version ultérieure, vous pouvez utiliser les paramètres de canal de notification gérer vos notifications par e-mail et calendrier. Cette fonctionnalité vous permet de personnaliser et de gérer vos notifications. Pour plus de détails, consultez la section Canaux de notification.
- **Signaler un e-mail de phishing (sous forme de transfert) :** dans Secure Mail pour iOS, vous pouvez utiliser la fonction Signaler comme phishing pour signaler un e-mail (sous forme de transfert) que vous soupçonnez de phishing. Vous pouvez transférer les messages suspects vers des adresses e-mail configurées par les administrateurs dans la stratégie. Pour activer cette fonctionnalité, un administrateur doit configurer la stratégie Signaler les adresses e-mail de phishing et définir **Mécanisme de signalisation de phishing** sur **Signaler via transfert**. Pour plus de détails, consultez la section Signaler un e-mail de phishing (sous forme de transfert).

**Secure Mail 18.9.0**

- Nouveau schéma de numérotation des versions au format "aa.mm.version". Par exemple, version **18.9.0**
- **Signaler un e-mail de phishing (sous forme de transfert) :** dans Secure Mail pour Android, vous pouvez utiliser la fonction Signaler comme phishing pour signaler un e-mail (sous forme de transfert) que vous soupçonnez de phishing. Vous pouvez transférer les messages suspects vers des adresses électroniques configurées par les administrateurs. Pour activer cette fonctionnalité, un administrateur doit configurer la stratégie Signaler les adresses e-mail de phishing et définir Mécanisme de signalisation de phishing sur **Signaler via transfert**. Pour plus de détails, consultez la section Signaler un e-mail de phishing (sous forme de transfert).

- **Améliorations des fiches de flux :** les améliorations suivantes ont été apportées au dossier **Flux** existant, dans Secure Mail pour Android :
  - Les invitations à des réunions provenant de tous les dossiers synchronisés automatiquement apparaissent dans votre fiche Flux.
  - Affichez jusqu'à cinq réunions à venir dans votre fiche Flux.
  - Les réunions à venir apparaissent désormais sur une période de 24 heures à compter de l'heure actuelle. Les invitations à ces réunions sont classées dans **Aujourd'hui** et **Demain**. Dans les versions précédentes, les réunions à venir jusqu'à la fin de la journée apparaissaient dans vos flux.
- **Exporter des événements de calendrier Secure Mail :** Secure Mail pour iOS et Android vous permet d'exporter des événements de calendrier depuis Secure Mail vers l'application de calendrier native de votre appareil. Pour activer cette fonctionnalité, touchez **Paramètres** et faites glisser le curseur Exporter événements du calendrier vers la droite. Pour plus de détails, voir Exporter des événements de calendrier Secure Mail.

**Secure Mail 10.8.65**

- **Disponible avec iOS 12 :** dans Secure Mail pour iOS, nous prenons en charge la fonctionnalité Notifications de groupe. Grâce à cette fonctionnalité, les conversations sont groupées dans un thread de courrier électronique. Vous pouvez consulter rapidement les notifications groupées sur l'écran de verrouillage de votre appareil. Les paramètres de notifications de groupe sont activés par défaut sur l'appareil.
- Dans Secure Mail pour iOS, les boutons **Enregistrer le brouillon** et **Supprimer le brouillon** sont plus gros. Cette amélioration permet aux clients de distinguer facilement une option de l'autre.
- Dans Secure Mail pour iOS, vous pouvez identifier les appels entrants à partir de vos contacts Secure Mail en activant Identification de l'appelant Secure Mail dans les **Réglages** de l'appareil. Lors de l'activation de ces paramètres, lorsque vous recevez un appel entrant, l'appareil affiche le nom de l'application avec l'ID de l'appelant, tel que « ID de l'appelant Secure Mail : Joe Jay ». Pour plus de détails, voir Identification de l'appelant Secure Mail.

**Secure Mail 10.8.60**

- Secure Mail prend en charge Android P.
- Secure Mail est maintenant disponible en polonais.
- Dans Secure Mail pour iOS, vous pouvez joindre des fichiers à votre e-mail à partir de l'application Fichiers native d'iOS. Pour plus de détails, voir Fonctionnalités iOS.

### Secure Mail 10.8.55

Il n'y a pas de nouvelles fonctionnalités dans Secure Mail version 10.8.55. Pour accéder aux problèmes résolus, veuillez consulter Problèmes connus et résolus.

### Secure Mail 10.8.50

**Améliorations au niveau de la pièce jointe photo** - Dans Secure Mail pour iOS, vous pouvez joindre facilement des photos en touchant la nouvelle icône **Galerie**. Touchez l'icône **Galerie** et sélectionnez les photos que vous souhaitez joindre à votre e-mail.

**Écran des flux Secure Mail**. Secure Mail pour iOS et Android proposent tous vos e-mails non lus, vos invitations à des réunions nécessitant votre attention et vos prochaines réunions dans l'écran **Flux**.

### Secure Mail 10.8.45

**Synchronisation des dossiers** - Dans Secure Mail pour iOS et Android, vous pouvez toucher l'icône **Synchroniser** pour actualiser tout le contenu de Secure Mail. L'icône **Synchroniser** est présente dans les menus contextuels de Secure Mail, telles que Boîtes aux lettres, Calendriers, Contacts et Pièces jointes. Lorsque vous touchez l'icône **Synchroniser**, les dossiers que vous avez configurés pour une actualisation automatique, tels que Boîtes aux lettres, Calendriers et Contacts, sont mis à jour. L'horodatage de la dernière synchronisation apparaît à côté de l'icône **Synchroniser**.

**Améliorations au niveau de la pièce jointe photo** - Dans Secure Mail pour Android, vous pouvez joindre facilement des photos en touchant la nouvelle icône **Galerie**. Touchez l'icône **Galerie** et sélectionnez les photos que vous souhaitez joindre à votre e-mail.

### Secure Mail 10.8.40

**Prise en charge de la recherche de calendrier -** Dans Secure Mail pour iOS, vous pouvez rechercher des événements, des participants ou tout autre texte dans le calendrier.

### Secure Mail 10.8.35

La version de Secure Mail pour iOS est 10.8.36.

- **Options de réponse de notification -** Dans Secure Mail pour iOS, les utilisateurs peuvent répondre aux notifications de réunion avec les options Accepter, Décliner et Provisoire. Ils peuvent répondre aux notifications de message avec les options Répondre et Supprimer.

- **Améliorations du bouton de retour dans Secure Mail pour Android** Dans Secure Mail pour Android, vous pouvez toucher le bouton de retour de votre appareil pour ignorer les options développées du bouton d'action flottant. Si le bouton d'action flottant est présenté dans l'état développé, touchez le bouton de retour de votre appareil pour réduire les options de réponse. Cette action vous ramène à la vue des détails du message ou de l'événement.
- **Dans Secure Mail pour Android, les boutons de réponse aux réunions apparaissent dans l'e-mail.** Lorsque vous recevez une notification par e-mail concernant une invitation à une réunion, vous pouvez répondre à l'invitation en touchant l'une des options suivantes :
  - Oui
  - Peut-être
  - Non

#### Secure Mail 10.8.25

**Secure Mail pour iOS prend désormais en charge S/MIME pour les informations d'identification dérivées**. Pour activer cette fonctionnalité, vous devez effectuer les opérations suivantes :

- Sélectionnez Informations d'identification dérivées comme source du certificat S/MIME. Pour de plus amples informations, consultez la section Informations d'identification dérivées pour iOS.
- Ajoutez la propriété client Attributs LDAP dans Citrix Endpoint Management. Utilisez les informations suivantes :
  - **Clé :** SEND_LDAP_ATTRIBUTES
  - **Valeur :** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme =${ user.samaccountname } ,displayName=${ user.displayName } ,mail= ${ user.mail }`

Pour plus d'informations sur l'ajout d'une propriété de client pour XenMobile Server, consultez la section Propriétés du client et pour Endpoint Management, la section Propriétés du client.

Pour plus d'informations sur l'inscription des appareils à l'aide d'informations d'identification dérivées, consultez la section Inscription à l'aide d'informations d'identification dérivées.

1. Dans la console Endpoint Management, accédez à **Configurer > Applications**.
2. Sélectionnez **Secure Mail**, puis cliquez sur **Modifier**.
3. Sous la plate-forme iOS, pour la source du certificat S/MIME, sélectionnez **Informations d'identification dérivées**.

**Secure Mail pour iOS et Android ont un aspect amélioré.** Nous avons simplifié et optimisé la navigation de l'utilisateur. Le menu Secure Mail et les boutons d'action ont été réalignés sous la forme d'une

barre de navigation. Pour plus d'informations sur les changements de navigation de l'utilisateur, visionnez la vidéo suivante :

L'illustration suivante montre la nouvelle barre de navigation sur les appareils iOS.

L'illustration suivante montre la nouvelle barre de navigation sur les appareils Android.

**Modifications :**

- L'icône de sélection a été supprimée. Les fonctions Secure Mail, telles que Boîte aux lettres, Calendrier, Contacts et Pièces jointes, sont maintenant disponibles en tant que boutons dans la barre d'onglets de pied de page. L'illustration suivante montre cette modification.

  > Remarque :
  >
  > Sur les appareils Android, la barre d'onglets de pied de page n'est pas disponible après l'ouverture d'un élément de messagerie. Par exemple, comme le montre l'illustration suivante, si vous ouvrez un e-mail ou un événement de calendrier, la barre d'onglets de pied de page n'est pas disponible.

- Le menu **Paramètres** est disponible dans tous les menus, tels que Courrier, Calendrier, Contacts et Pièces jointes. Pour accéder à **Paramètres**, touchez l'icône d'hamburger, puis touchez le bouton des paramètres disponible en bas à droite, comme indiqué dans l'illustration suivante.
- L'icône de **recherche** remplace la barre de recherche et est disponible dans les vues Boîte de réception, Contacts et Pièces jointes.
- Sur les appareils iOS, vous pouvez toucher et maintenir un élément de messagerie pour le sélectionner.
- Vous pouvez toucher le bouton d'action flottant **Rédiger** pour composer un nouvel e-mail, comme indiqué dans l'illustration suivante.
- Les options de menu suivantes sont maintenant disponibles en haut à droite de votre écran :
  - **Options de synchronisation :** touchez l'icône de débordement en haut à droite et accédez à **Plus d'options > Options de synchronisation** pour modifier vos préférences de synchronisation.

    > **Remarque :**
    >
    > Cette option est disponible uniquement sur les appareils Android.

  - **Icône de recherche :** touchez cette icône pour rechercher un e-mail.
- **Icône de vue de triage :** touchez cette icône sur pour afficher le triage de la conversation.
- **Bouton d'action flottant Répondre :** lorsque vous consultez un e-mail, touchez Transférer, Répondre à tous ou Répondre, comme indiqué dans l'illustration suivante.

- Lorsque vous consultez un e-mail, les options de menu suivantes sont disponibles en haut à droite de votre écran :
  - **Drapeau :** touchez cette option pour marquer l'e-mail d'un drapeau.
  - **Marquer comme non lu :** touchez cette option pour marquer l'e-mail comme non lu.
  - **Supprimer :** touchez cette option pour supprimer l'e-mail.
  - **Plus d'options :** touchez l'icône de débordement pour afficher d'autres actions disponibles, telles que Déplacer.

**Modifications au niveau du calendrier**

- À partir du calendrier, vous pouvez toucher un bouton d'action flottant pour créer un événement, comme indiqué dans l'illustration suivante.
- Les options de menu suivantes sont maintenant disponibles en haut à droite de votre écran :
  - **Aujourd'hui :** touchez cette option pour afficher les événements d'aujourd'hui.
  - **Rechercher :** touchez cette option pour rechercher un événement.
  - **Bouton d'action flottant Répondre :** lorsque vous consultez un e-mail, touchez Transférer, Répondre à tous ou Répondre pour effectuer l'action correspondante.

Lorsque vous affichez un événement, les actions de réponse aux événements telles que Oui, Peut-être et Non sont réalignées et disponibles sous les détails de l'événement.

**Modifications au niveau des contacts**

- Vous pouvez toucher le bouton d'action flottant **Créer un nouveau contact**, comme indiqué dans l'illustration suivante.
- L'option de menu **Rechercher** est maintenant disponible en haut à droite de l'écran. Vous pouvez toucher cette option pour rechercher un contact.
- Lorsque vous affichez un contact, les options de menu suivantes sont disponibles en haut à droite de votre écran :

  **Sur les appareils Android :**

  - **Modifier :** touchez cette option pour modifier le contact.
  - **Plus d'options :** touchez l'icône de modification pour afficher d'autres actions disponibles, telles que Joindre au message, Partager et Supprimer.

  **Sur les appareils iOS :**

  - **Modifier :** touchez cette option pour modifier le contact.
  - **Partager :** touchez l'icône de partage pour afficher d'autres actions disponibles, telles que Partager contact et Joindre au message.

> **Remarque :**
>
> Pour supprimer un contact sur les appareils iOS, sélectionnez le contact, touchez **Modifier**, puis **Supprimer** en bas de l'écran, comme indiqué dans l'illustration suivante.

#### Modifications au niveau des pièces jointes

Les options de menu suivantes pour les pièces jointes sont maintenant disponibles en haut à droite de votre écran :

- **Trier :** touchez l'icône **Trier** et choisissez les filtres appropriés pour trier les pièces jointes.
- **Rechercher :** touchez cette option pour rechercher une pièce jointe.

### Secure Mail 10.8.20

- Secure Mail pour iOS prend désormais en charge l'utilisation d'informations d'identification dérivées pour l'inscription et l'authentification. Pour de plus amples informations, consultez la section Informations d'identification dérivées pour iOS.
- Secure Mail pour iOS prend en charge les notifications Push enrichies. Grâce aux notifications enrichies, vous recevez des notifications d'écran de verrouillage pour votre boîte de réception même lorsque Secure Mail n'est pas exécuté en arrière-plan. Cette fonctionnalité est prise en charge avec les configurations d'authentification par mot de passe et d'authentification basée sur le client. Pour plus d'informations, consultez la section Notifications push enrichies.

  > Remarque :
  >
  > En raison de la modification de l'architecture pour prendre en charge la fonction de notifications push enrichies, les notifications par e-mail **VIP uniquement** ne sont plus disponibles.

- Secure Mail pour Android et iOS prend désormais en charge les signatures au format RTF. Vous pouvez utiliser des images ou des liens dans votre signature électronique. Pour plus de détails, voir Signatures au format RTF.

### Secure Mail 10.8.15

- **Secure Mail pour iOS prend désormais en charge les signatures au format RTF.** Vous pouvez utiliser des images ou des liens dans votre signature électronique. Pour plus de détails, voir Signatures au format RTF.
- **Secure Mail prend en charge Android Enterprise, anciennement appelé Android for Work**. Vous pouvez créer un profil de travail séparé à l'aide d'applications d'entreprise Android dans

Secure Mail. Pour de plus amples informations, consultez la section Android Entreprise dans Secure Mail.

- **Secure Mail affiche les ressources intégrées lors de l'affichage d'un e-mail.** Si les ressources sont présentes dans votre réseau interne, telles que des e-mails avec des adresses URL d'image qui sont des liens internes, Secure Mail se connecte vers le réseau interne pour récupérer le contenu et le restituer.
- **Secure Mail prend en charge l'authentification moderne**. L'authentification moderne est une authentification basée sur un jeton OAuth avec nom d'utilisateur et mot de passe. Cette prise en charge inclut la gestion d'Office 365 pour les services AD FS (Active Directory Federation Services) internes et externes, ainsi que le fournisseur d'identité (IdP).
- **Amélioration des performances sur le référentiel de pièces jointes**. Vous pouvez parcourir votre référentiel de pièces jointes beaucoup plus rapidement.

#### Secure Mail 10.8.10

- **Prise en charge de l'impression des pièces jointes**. Secure Mail pour iOS prend en charge l'impression des pièces jointes.
- **Authentification moderne à l'aide de Microsoft Office 365**. Secure Mail pour iOS prend en charge l'authentification moderne. L'authentification moderne est une authentification basée sur un jeton OAuth avec nom d'utilisateur et mot de passe. Cette prise en charge inclut la gestion d'Office 365 pour les services AD FS (Active Directory Federation Services) internes et externes, ainsi que le fournisseur d'identité (IdP).

  > Remarques :
  >
  > – Cette version ne prend pas en charge l'authentification moderne avec l'intégration Endpoint Management avec Microsoft Intune/EMS.
  > – Cette version comprend l'authentification moderne dans un scénario dans lequel AD FS est accessible en externe.

  Pour de plus amples informations, consultez la section Authentification moderne à l'aide de Microsoft Office 365.

## Problèmes connus et résolus

March 1, 2019

Cet article traite également des problèmes liés à MDX qui affectent Secure Mail.

## Problèmes connus dans la version 19.2.0

Il n'existe pas de problème connu dans la version 19.2.0.

## Problèmes résolus dans la version 19.2.0

### Secure Mail pour iOS

Dans Secure Mail pour iOS, vous ne pouvez pas copier le texte du champ objet de Secure Mail vers Secure Notes 10.8.6.6. [CXM-61060]

### Secure Mail pour Android

- Dans Secure Mail pour Android, si le texte prédictif est activé sur les appareils Samsung, le dernier mot du texte est souligné. Le dernier mot de la signature est enregistré avec un soulignement lorsque vous ne laissez pas d'espace, et le destinataire peut le voir aussi. [CXM-60894]
- Dans Secure Mail pour Android, lorsque vous recevez un récapitulatif d'e-mail, les images ne sont pas affichées. [CXM-62280]
- Secure Mail pour Android se bloque au lancement lorsque Intune Company Portal version 5.0.4324.0 est installé. Pour plus de détails, consultez cet article du centre de connaissances. [CXM-62516]

## Problèmes connus et résolus dans Secure Mail pour iOS version 19.1.6

Il n'existe aucun problème connu dans la version 19.1.6.

### Problèmes résolus dans les versions précédentes

Les problèmes suivants ont été résolus dans les versions précédentes :

## Problèmes connus dans la version 19.1.5

Il n'y a aucun problème connu dans la version 19.1.5.

## Problèmes résolus dans la version 19.1.5

Les problèmes suivants ont été résolus dans la version 19.1.5 :

- Dans Secure Mail pour iOS, le message d'erreur suivant s'affiche pour chaque courrier que vous recevez : **Impossible de récupérer ce message. Veuillez ouvrir Secure Mail** [CXM-56418]
- Dans Secure Mail pour iOS, vous obtenez fréquemment le message d'erreur Réseau d'entreprise indisponible, lors de l'ouverture de l'application et de la saisie du code PIN. [CXM-59766]
- Dans les applications Android encapsulées, la chaîne UserAgent est ajoutée plusieurs fois, ce qui entraîne une augmentation de la taille de l'en-tête. Ce comportement entraîne une erreur et la page ne parvient pas à se charger. [CXM-59869]

### Problèmes résolus dans la version 19.1.0

#### Secure Mail pour iOS

- Lorsque Secure Mail ne parvient pas à se connecter à Exchange Server, le message suivant apparaît sur la bannière de notification par e-mail :

  Nous ne pouvons pas récupérer ce message car votre session a expiré. Ouvrez Secure Mail pour renouveler votre session.

  Ce problème a été résolu et le message a été mis à jour comme suit :

  « Secure Mail ne peut pas se connecter au réseau de votre entreprise. Veuillez contacter votre administrateur. » [CXM-59128]

- Pour les utilisateurs exécutant des boîtes aux lettres O365, l'exécution répétée d'actions de réponse de notification telles que **Oui, Non, Peut-être ou Supprimer** entraîne une limitation de bande passante d'Office 365 et le message d'erreur suivant :

  « Le serveur est occupé. Veuillez réessayer. » [CXM-60123]

#### Secure Mail pour Android

- Dans Secure Mail pour Android, si vous utilisez la langue turque, vous ne pouvez pas envoyer d'e-mails aux destinataires dont l'adresse contient le caractère « I ». [CXM-59093]
- Dans Secure Mail pour Android, les utilisateurs ne peuvent pas sélectionner et surligner la ligne d'objet d'un e-mail. [CXM-59185]
- Dans Secure Mail pour Android, l'ouverture de session échoue si le mot de passe contient le caractère €. [CXM-59654]
- Dans Secure Mail pour Android, lorsque le paramètre **Synchroniser avec les contacts locaux** est activé, tous vos contacts Secure Mail sont exportés vers vos contacts natifs. Après la synchronisation, les champs de téléphone tels que mobile, bureau, domicile, télécopie bureau et télécopie domicile, n'apparaissent pas dans l'ordre correct. Par exemple, dans vos contacts natifs, le numéro de télécopie apparaît au-dessus du numéro de téléphone mobile. Les utilisateurs ne peuvent pas modifier cet ordre. [CXM-57994]

### Problèmes résolus dans la version 18.12.0

#### Secure Mail pour iOS

- Dans Secure Mail pour iOS, lorsque vous recevez un courrier au format RTF, certains types de pièces jointes en ligne et le symbole de pièce jointe ne sont pas visibles. [CXM-59121]
- Dans Secure Mail pour iOS, lorsque les notifications push enrichies sont activées et que vous désactivez et activez les **notifications par e-mail**, l'option **Type de message** s'affiche par intermittence. [CXM-59122]

#### Secure Mail pour Android

- Si vous exécutez le mécanisme d'authentification basée sur le client dans votre environnement, Secure Mail ne peut pas synchroniser automatiquement les e-mails par intermittence. L'exécution d'une synchronisation manuelle ne récupère que quelques e-mails. [CXM-59650]

### Problème résolu dans la version 18.11.1

- Dans Secure Mail pour Android avec des connexions à IBM Notes Traveler 9.0.1 SP 10, les e-mails avec pièces jointes restent dans la boîte d'envoi. [CXM-58962]

### Problèmes résolus dans la version 18.11.0

- Dans Secure Mail pour Android, les images incorporées ne sont pas visibles dans un e-mail. [CXM-53556]
- Secure Mail pour Android se bloque lors de l'ouverture d'un e-mail dont la signature contient une URL intégrée, telle que `file://C:\...jpg`. [CXM-58219]

### Problèmes résolus dans la version 18.10.5

#### Secure Mail pour iOS

- Lorsque la stratégie MDX Activer la protection des données iOS est activée, vous recevez la notification « Vous avez un nouvel e-mail » par intermittence. [CXM-55491]
- Sur l'iPhone XS, les pièces jointes ne peuvent pas être téléchargées ou envoyées et les images téléchargées ne peuvent pas être affichées. [CXM-57030]

#### Secure Mail pour Android

- Lorsque les utilisateurs modifient une réunion périodique pour les comptes exécutant Exchange ActiveSync version 16 et ultérieure, la réunion ne se met pas à jour dans Exchange Server. Par conséquent, la réunion n'est pas synchronisée entre Secure Mail et Outlook. [CXM-57200]

#### Problèmes résolus dans la version 18.10.0

- Dans Secure Mail pour Android, les utilisateurs ne peuvent pas afficher les images en ligne qui pointent vers des serveurs autres que les serveurs Exchange. [CXM-56736] [CXM-55843]
- Dans Secure Mail pour Android, le numéro PIN n'était pas ajouté au numéro à composer lors de la participation à des réunions Webex. Vous deviez taper le code PIN manuellement. [CXM-56002]
- Secure Mail pour Android se bloque lors de la tentative d'exportation du calendrier Secure Mail si votre calendrier personnel n'est pas configuré. [CXM-56264]
- Sur l'iPhone XS, dans Secure Mail pour iOS, les pièces jointes ne peuvent pas être téléchargées ou envoyées et les images téléchargées ne peuvent pas être affichées. [CXM-57030]

#### Problèmes résolus dans la version 18.9.0

##### Secure Mail pour Android

- Le poste de travail client change de manière aléatoire avec chaque demande d'authentification NT LAN Manager (NTLM). [CXM-55177]
- La synchronisation de Secure Mail sur Android P cesse de fonctionner par intermittence lorsque l'appareil est en mode d'économie de batterie. [CXM-55441]
- Secure Mail se bloque lors de la tentative d'exportation du calendrier Secure Mail si votre calendrier personnel n'est pas configuré. [CXM-56264]

#### Problèmes résolus dans la version 10.8.65

##### Secure Mail pour iOS

- Lorsque FIP est activé et que les utilisateurs exécutent Secure Mail pour iOS sur un appareil iOS 11.3, les stratégies Couper et copier et Coller MDX ne fonctionnent pas comme prévu. [CXM-53993]
- Lors de l'utilisation de Secure Mail pour iOS sur des appareils partagés, les nouveaux utilisateurs peuvent afficher les e-mails d'un utilisateur précédent même si cet utilisateur s'était déconnecté. Si le nouvel utilisateur appuie sur un dossier pour actualiser l'affichage, les e-mails des utilisateurs précédents n'apparaissent plus. [CXM-55176]

**Problèmes résolus dans la version 10.8.60**

> Remarque :
>
> Les versions 10.8.25 à 10.8.60 de Secure Mail ne comprennent aucun problème connu.

- Dans Secure Mail pour iOS exécuté sur des serveurs IBM Lotus Domino, vous ne pouvez pas utiliser l'icône de recherche dans votre boîte de réception. [CXM-53782]
- Lorsque les utilisateurs inscrivent un appareil exécutant Secure Mail pour Android avec le portail d'entreprise Intune, Secure Mail cesse de fonctionner. [CXM-54178]
- Secure Mail pour iOS se bloque lors de la synchronisation d'un grand nombre de dossiers de messagerie à partir du serveur au cours d'un flux FTU. [CXM-54371]
- Dans Secure Mail pour iOS, l'aperçu avant impression des PDF semble plus petit. [CXM-54482]
- Dans Secure Mail pour Android, plusieurs ID de messagerie ne sont pas automatiquement renseignés lors de la réponse à des e-mails. [CXM-54811]

**Problèmes résolus dans la version 10.8.55**

- Dans Secure Mail pour iOS, la vue hebdomadaire du calendrier est affichée de manière incorrecte en mode paysage sur un iPad Pro. [CXM-53723]

**Problèmes résolus liés à MDX dans la version 10.8.55**

- Sur Android, Secure Mail se bloque lorsque les utilisateurs sont déconnectés de Secure Hub. [CXM-53930]
- Sur les appareils iOS, Secure Web et Secure Mail 10.8.45 se bloquent au lancement. [CXM-54089]

**Problèmes résolus dans la version 10.8.50**

- Secure Mail pour iOS ne peut pas enregistrer de fichiers vidéo sur ShareFile. [CXM-42238]
- Lorsque vous activez les notifications push dans Secure Mail pour Android, vous ne recevez pas de notifications pour les nouveaux messages. Ce problème se produit par intermittence. [CXM-53135]

**Problèmes résolus dans la version 10.8.45**

Secure Mail version 10.8.45 ne comprenait aucun problème résolu.

**Problèmes résolus dans la version 10.8.40**

Dans Secure Mail pour iOS, une notification dupliquée s'affiche par intermittence pour chaque nouvel e-mail que vous recevez. [CXM-51473]

**Problèmes résolus dans la version 10.8.35**

- Dans Secure Mail pour Android, la synchronisation automatique s'arrête par intermittence. Les utilisateurs doivent effectuer la synchronisation manuellement pour que certains nouveaux messages des serveurs Office 365 apparaissent dans Secure Mail. [CXM-49354, CXM-52716]
- Dans Secure Mail pour Android, même si vous désactivez les notifications par e-mail dans Secure Mail pour les événements de messagerie et de calendrier, les notifications apparaissent toujours et une notification sonore se produit. [CXM-50479]
- Lorsque vous créez un événement de type Toute la journée à l'aide de Secure Mail pour Android, des dates incorrectes s'affichent dans votre calendrier Outlook. [CXM-50612]
- Dans Secure Mail pour Android, les groupes de contacts personnels Exchange ne sont pas synchronisés avec l'application. [CXM-51190]
- Lorsque SSO est configuré, Secure Mail pour Android SSO à Exchange échoue. Les utilisateurs sont invités à entrer un mot de passe. [CXM-51343]

**Problèmes résolus dans la version 10.8.25**

- Dans Secure Mail pour Android, un délai se produit lorsque les utilisateurs synchronisent une invitation de calendrier avec Office 365. Le problème se produit lors de la création ou de la mise à jour d'une invitation de calendrier. [CXM-49596]
- Dans Secure Mail pour Android, lorsque les utilisateurs tapent une seule lettre dans le champ Cc : puis touchent **Envoyer**, Secure Mail envoie le message au premier utilisateur de la liste des utilisateurs fréquemment utilisés. Au lieu de cela, une notification devrait apparaître indiquant que l'entrée du champ Cc : n'est pas valide. [CXM-50476]
- Sur les appareils Zebra T51 fonctionnant sous Android 7, les utilisateurs ne peuvent pas installer l'application Citrix Launcher. [CXM-50621]
- Lorsque NetScaler Gateway est configuré avec l'authentification par certificat : dans Secure Mail pour iOS, chaque fois que les utilisateurs reçoivent un nouveau message, le message « Vous avez nouveau message » s'affiche. Au lieu de cela, la notification devrait répertorier le nom de l'expéditeur, l'objet et l'aperçu du corps. [CXM-51075]

**Problèmes résolus dans la version 10.8.20**

- Si l'application Intune Company Portal est installée sur les appareils Android inscrits en mode MAM uniquement, dans Endpoint Management, Secure Mail tente une redirection vers la page de connexion Microsoft. Le message d'erreur suivant s'affiche : Aucune configuration reçue pour l'application. Contactez votre administrateur pour configurer l'application. [CXM-48135]
- Dans Secure Mail pour Android, la connexion échoue si votre nom d'utilisateur ou votre mot de passe contient des caractères spéciaux tels que ä, ö, ü ou €. [CXM-48197]
- Sur les appareils Android, un redémarrage vous permet de contourner l'authentification pour accéder à Secure Mail. [CXM-48444]
- Dans Secure Mail pour Android, lorsque vous répondez à des e-mails avant le téléchargement des images en ligne, les e-mails sont bloqués dans votre boîte d'envoi. Ce problème se produit lorsque le paramètre **Afficher les images** est activé dans vos paramètres. [CXM-49222]
- Dans Secure Mail pour iOS, si la stratégie IRM est **activée** et que la classification des e-mails est définie sur **Protégé**, vous ne pouvez pas afficher les pièces jointes lorsque vous téléchargez le courrier complet. [CXM-49544]

**Problèmes résolus dans la version 10.8.10**

**Secure Mail pour iOS**

- Après la mise à jour vers Secure Mail 10.7.25 pour iOS, les crochets sont absents de l'en-tête Message-ID (< et >). [CXM-46029]
- Dans Secure Mail pour iOS, après que les utilisateurs ont ajouté une invitation au calendrier depuis Outlook, l'application se bloque par intermittence. Ce problème se produit si votre invitation de calendrier contient un Emoji. [CXM-46250]
- Sur iOS, après la mise à niveau des applications de productivité mobiles vers la version 10.7.30, si le niveau de journalisation est défini sur 11 ou plus, Secure Mail est lent et se bloque s'il reste ouvert. [CXM-46721]
- Dans Secure Mail pour iOS, des notifications en double s'affichent par intermittence si la stratégie Contrôler les notifications de l'écran verrouillé est définie sur **Nombre uniquement**. [CXM-47461]

**Secure Mail pour Android**

Dans Secure Mail pour Android, lorsque les utilisateurs copient et collent quatre adresses e-mail ou plus dans le champ À:, l'application se bloque. [CXM-46578]

### Problèmes connus dans la version actuelle

Il n'existe pas de problèmes connus dans la version 19.1.0

### Problèmes connus dans les versions précédentes

Il n'existe pas de problèmes connus dans les versions 10.8.65 à 18.11.5.

#### Problèmes connus dans la version 18.11.5

- Il n'y a aucun problème connu dans la version 18.11.5.

## Déploiement de Secure Mail

March 1, 2019

Pour déployer Secure Mail avec Citrix Endpoint Management (anciennement XenMobile), procédez comme suit :

1. Vous pouvez intégrer Secure Mail avec un serveur Exchange ou IBM Notes Traveler afin de garder Secure Mail synchronisé avec Microsoft Exchange ou IBM Notes. Si vous utilisez IBM Notes, configurez le serveur IBM Notes Traveler. La configuration utilise les informations d'identification Active Directory pour s'authentifier auprès d'Exchange ou du serveur IBM Notes Traveler. Pour de plus amples informations, consultez la section Intégration à un serveur Exchange ou un serveur IBM Notes Traveler.

   > **Important :**
   >
   > Vous ne pouvez pas synchroniser la messagerie à partir de Secure Mail avec IBM Notes Traveler (anciennement IBM Lotus Notes Traveler). Cette fonctionnalité tierce Lotus Notes n'est actuellement pas prise en charge. Par conséquent, lorsque vous supprimez un message de réponse à une réunion à partir de Secure Mail, le message n'est pas supprimé sur le serveur IBM Notes Traveler. Si les utilisateurs acceptent un événement de calendrier et le refusent ensuite avec un commentaire ou qu'ils répondent à un commentaire, le commentaire est manquant. [CXM-47936] Pour en savoir plus sur les limitations avec IBM/Lotus Notes, veuillez consulter ce billet de blog Citrix.

2. Vous pouvez également activer l'authentification unique (SSO) à partir de Secure Hub. Pour ce faire, vous configurez les informations de compte Citrix Files dans la console Endpoint Management afin d'activer Endpoint Management en tant que fournisseur d'identité SAML pour Citrix Files. La configuration utilise les informations d'identification Active Directory pour s'authentifier auprès de Citrix Files.

La configuration des informations du compte Citrix Files dans la console Endpoint Management ne doit être effectuée qu'une seule fois pour tous les clients Citrix, clients Citrix Files et clients Citrix Files non-MDX. Pour plus de détails, voir Pour configurer les informations de compte Citrix Files dans la console Endpoint Management pour SSO.

3. Téléchargez le fichier .mdx Secure Mail depuis le site de téléchargement de Citrix.
4. Ajoutez Secure Mail à Endpoint Management et configurez les stratégies MDX. Pour de plus amples informations, consultez la section [Ajouter des applications].(/fr-fr/citrix-endpoint-management/apps.html)

> Remarque :
>
> À compter de la version 10.6.5 de Secure Mail, vous pouvez configurer une nouvelle stratégie d'analyse de MDX pour Secure Mail pour iOS et Android. Citrix collecte des données d'analyse pour améliorer la qualité de ses produits. Le niveau de détail de la stratégie Google Analytics vous permet de spécifier si les données sont associées au domaine de votre entreprise ou collectées de façon anonyme. Si l'option **anonyme** est sélectionnée, les utilisateurs n'ont pas besoin d'inclure le domaine d'entreprise avec les données qui sont collectées. Cette nouvelle stratégie remplace une stratégie Google Analytics antérieure.

Lorsque la stratégie est définie sur anonyme, nous collectons les types de données suivants. Nous n'avons absolument aucun moyen de lier ces données à un utilisateur ou à une entreprise car nous ne demandons aucune information identifiable de l'utilisateur. Aucune information permettant de vous identifier personnellement n'est envoyée à Google.

- Statistiques de l'appareil, telles que la version du système d'exploitation, la version de l'application et le modèle de l'appareil
- Informations sur la plate-forme, telles que la version ActiveSync et la version du serveur Secure Mail
- Points d'échec pour la qualité du produit, tels que les enregistrements APN, la synchronisation et l'envoi du courrier, le téléchargement des pièces jointes et la synchronisation du calendrier.

Aucune information identifiable autre que le domaine d'entreprise n'est collectée lorsque la stratégie est définie sur l'option **complète**. Le paramètre par défaut est **Complète**.

## Configuration de Secure Mail

February 11, 2019

Les fonctionnalités suivantes peuvent être configurées et intégrées dans Secure Mail :

- Intégration de Secure Mail avec Microsoft Intune/EMS
- Authentification moderne à l'aide d'Office 365

- Services d'arrière-plan pour Secure Mail
- Intégration à un serveur Exchange Server ou un serveur IBM Notes Traveler
- S/MIME pour Secure Mail
- SSO pour Secure Mail

## Intégration de Secure Mail avec Microsoft Intune/EMS

February 19, 2019

Grâce à cette intégration, vous pouvez gérer et mettre à disposition Citrix Secure Mail avec davantage de sécurité tout en améliorant la productivité.

Secure Mail prend en charge diverses configurations Intune. Vous pouvez connecter Secure Mail à des boîtes aux lettres locales Exchange ou Office 365. Pour configurer l'intégration de Endpoint Management avec Microsoft Intune/EMS, consultez Intégration de Citrix Endpoint Management avec Microsoft Intune/EMS

Secure Mail prend en charge les modes de déploiement suivants :

- Gestion des applications mobiles (MAM) Intune
- Gestion des applications mobiles (MAM) et gestion des appareils mobiles (MDM) Intune
- Gestion des applications mobiles (MAM) Intune avec Endpoint Management en mode MDM exclusif
- Gestion des applications mobiles (MAM) Intune avec Endpoint Management en mode MDM et MAM

### Serveurs de messagerie pris en charge

- Exchange Online
- Exchange Server 2016
- Exchange Server 2013

### Limitations

Secure Mail ne prend pas en charge l'authentification basée sur certificats.

> **Important :**
>
> Pour utiliser Secure Mail en mode MDM avec Citrix Endpoint Management (MDM et MAM), vous devez configurer Secure Hub dans votre environnement.

**Pour configurer Secure Mail pour Intune**

Si votre environnement est configuré en mode Citrix Endpoint Management MDM, Secure Mail renseigne automatiquement les noms d'utilisateur lors de la première utilisation.

Pour activer cette fonctionnalité, vous devez configurer des stratégies personnalisées dans la console Endpoint Management. Pour plus de détails, consultez la documentation de Endpoint Management, Pour configurer Secure Mail.

### Fonctionnalités incompatibles avec Intune

Les fonctionnalités Secure Mail suivantes ne sont pas compatibles avec l'intégration Endpoint Management avec EMS/Intune :

- Secure Ticket Authority
- Inscription à la messagerie à l'aide de l'authentification unique (Single Sign-On)
- Notifications push enrichies
- Citrix Files (anciennement ShareFile)
- Signature et cryptage S/MIME
- Gestion des droits relatifs à l'information Microsoft
- Navigation sécurisée + serveur Exchange interne SSO non KCD

## Authentification moderne à l'aide de Microsoft Office 365

February 11, 2019

Secure Mail prend en charge l'authentification moderne à l'aide de Microsoft Office 365 pour Active Directory Federation Services (ADFS) ou pour un fournisseur d'identité (IdP). L'authentification moderne est une authentification basée sur un jeton OAuth avec nom d'utilisateur et mot de passe. Les utilisateurs Secure Mail équipés d'appareils iOS peuvent bénéficier de l'authentification basée sur les certificats pour se connecter à Office 365. Lorsqu'ils se connectent à Secure Mail, les utilisateurs s'authentifient à l'aide d'un certificat client, au lieu de taper leurs informations d'identification.

Avant de continuer, procédez comme suit :

1. Activez l'authentification moderne (OAuth) pour Microsoft Office 365.
2. Activez les points de terminaison Office 365, les URL et les plages d'adresses IP dans votre pare-feu pour garantir une connectivité réseau optimale. Pour plus de détails, consultez la documentation Microsoft sur les URL et plages d'adresses IP Office 365.

### Conditions préalables de la stratégie Citrix Endpoint Management

Activez les stratégies suivantes dans la console Citrix Endpoint Management :

**Pour les appareils fonctionnant sous iOS :**

- **Mécanisme d'authentification Office 365 :** utilisez cette stratégie pour spécifier le mécanisme OAuth utilisé pour l'authentification lors de la configuration d'un compte sur Office 365. Cette stratégie comporte les valeurs suivantes que vous devez configurer :
  - **Ne pas utiliser OAuth :** utilisez cette stratégie pour l'authentification de base lors de la configuration du compte.
  - **Utiliser OAuth avec nom d'utilisateur et mot de passe :** utilisez cette stratégie pour le protocole OAuth lors de l'authentification. Les utilisateurs doivent fournir leur nom d'utilisateur et leur mot de passe, et éventuellement un code d'authentification à plusieurs facteurs pour le flux OAuth.
  - **Utiliser OAuth avec certificat client :** utilisez cette stratégie si Office 365 est configuré pour effectuer une authentification basée sur un certificat. La configuration par défaut est **Ne pas utiliser OAuth**.

**Pour les appareils fonctionnant sous Android :**

- **Utiliser l'authentification moderne pour O365 :** utilisez cette stratégie pour le protocole OAuth lors de l'authentification.
- **Agent utilisateur personnalisé pour l'authentification moderne :** utilisez cette stratégie pour modifier la chaîne de l'agent utilisateur par défaut pour l'authentification moderne.

**Stratégies communes aux appareils iOS et Android :**

- **Noms d'hôte Exchange Online approuvés :** utilisez cette stratégie pour définir une liste de noms d'hôtes Exchange Online approuvés qui utilisent le mécanisme OAuth pour l'authentification lors de la configuration d'un compte. Il s'agit d'un format séparé par des virgules, tel que serveur.entreprise.com, serveur.entreprise.fr. Cette liste peut contenir une valeur par défaut ou des URL de redirection vers un microsite, mais ne peut pas être vide. La valeur par défaut est **outlook.office365.com**.
- **Noms d'hôte AD FS de confiance :** utilisez cette stratégie pour définir une liste de noms d'hôte AD FS approuvés pour les pages Web où le mot de passe est renseigné lors de l'authentification OAuth Office 365. Il s'agit d'un format séparé par des virgules, tel que `sts.companyname.com` , `sts.company.co.uk`. Si la liste est vide, Secure Mail ne remplit pas automatiquement les mots de passe. Secure Mail fait correspondre les noms d'hôte répertoriés au nom d'hôte de la page Web rencontré lors de l'authentification Office 365 et vérifie si la page utilise le protocole HTTPS. Par exemple, lorsque `sts.company.com` est un nom d'hôte répertorié, si l'utilisateur accède à `https://sts.company.com`, Secure Mail remplit le mot de passe si la page comporte un champ de mot de passe. La valeur par défaut est `login.microsoftonline.com`.

- **Serveur Exchange Secure Mail :** utilisez cette stratégie pour définir l'adresse de votre serveur Exchange Server.

Secure Mail pour iOS est maintenant activé avec l'authentification moderne une fois les stratégies actualisées sur l'appareil.

## Limitations

- Si vous utilisez l'authentification moderne dans votre environnement, la fonctionnalité de notifications push enrichies pour iOS n'est pas disponible. Pour plus de détails sur les notifications push enrichies, consultez la section Notifications push pour Secure Mail.
- Plusieurs comptes ne sont pas pris en charge sur les configurations exécutant l'authentification basée sur les certificats.

### Stratégies Secure Mail

Les deux tableaux suivants répertorient les stratégies Secure Mail requises en fonction de votre infrastructure Exchange :

| Infrastructure Exchange | Mécanisme d'authentification Office 365/Utiliser l'authentification moderne pour O365 | Noms d'hôte ADFS de confiance | Noms d'hôte Exchange Online approuvés |
|---|---|---|---|
| Local | OFF | SO | SO |
| Hybride* | ON | ADFS/IDP | `Outlook.office365.com` ou URL de redirection vers un microsite |
| Exchange Online | ON | ADFS/IDP | `Outlook.office365.com` ou URL de redirection vers un microsite |

| Infrastructure Exchange | Serveur Exchange Secure Mail | Services réseau d'arrière-plan (iOS) | Services réseau d'arrière-plan (Android) |
|---|---|---|---|
| Local | Nom d'hôte Exchange local | Local | Local |
| Hybride* | Local, noms d'hôte Exchange Online | Local, Nom d'hôte local Exchange | Local, nom d'hôte Exchange local, AD FS/IDP (interne uniquement) |
| Exchange Online | `Outlook.office365.com` | Noms d'hôte Exchange Online | Nom d'hôte Exchange local, ADFS, IDP |

* Secure Mail prend en charge une infrastructure Exchange hybride avec des boîtes aux lettres migrées.

Si la boîte aux lettres des utilisateurs locaux est migrée vers Exchange Online, Secure Mail détecte automatiquement cette modification et invite les utilisateurs à utiliser une authentification moderne sans avoir à reconfigurer leur compte.

> **Remarque :**
>
> Configurez les services réseau d'arrière-plan uniquement si votre serveur de messagerie et ADFS sont internes.

**Secure Mail avec matrice de prise en charge OAuth**

Le tableau suivant répertorie la matrice de prise en charge de Secure Mail OAuth sur les appareils iOS et Android :

| Type d'authentification | IDP/ADFS externe | IDP/ADFS interne | Azure AD | Intune |
|---|---|---|---|---|
| Nom d'utilisateur et mot de passe | Oui | Oui | Oui | Oui |
| Certificat client | Oui | Android uniquement | Non | Non |

# Services d'arrière-plan pour Secure Mail

March 1, 2019

Pour accéder à votre serveur de messagerie via Citrix Gateway, vous devez configurer les services d'arrière-plan pour Secure Mail. Lorsque vous ajoutez Secure Mail à Citrix Endpoint Management (anciennement XenMobile), configurez les services d'arrière-plan dans les paramètres de stratégies d'application MDX.

## Configurer les services d'arrière-plan pour Secure Mail

1. Ouvrez une session sur la console Endpoint Management à l'aide des informations d'identification de l'administrateur.
2. Dans la console, cliquez sur l'onglet **Configurer**, sur **Applications**, sélectionnez l'application Secure Mail, puis cliquez sur **Modifier**.
3. Sur la page des **paramètres de stratégie MDX**, dans la section **Plate-forme**, sélectionnez la plate-forme iOS ou Android selon vos besoins.
4. Dans la section **Paramètres d'application**, configurez les stratégies.

## Stratégies d'application MDX pour la configuration des services d'arrière-plan

Les stratégies d'application MDX suivantes affectent la communication de Secure Mail avec Citrix Gateway, le serveur Citrix Endpoint Management, les serveurs STA (Secure Ticket Authority) et le serveur de messagerie.

**Accès réseau :** la stratégie d'accès réseau spécifie si Secure Mail peut utiliser un VPN pour accéder aux services réseau d'arrière-plan ou si tout le trafic passe sans restriction via cet Internet.

- Si la stratégie d'accès réseau est définie sur **Tunnélisé vers le réseau interne**, seules les URL répertoriées dans les services réseau d'arrière-plan passent par Citrix Gateway. Le reste du trafic n'est pas limité via Internet. Par défaut, l'accès Secure Mail est défini sur **Tunnélisé vers le réseau interne**.
- Si la stratégie d'accès réseau est définie sur **Non restreint**, tout le trafic provenant de Secure Mail est envoyé sans restriction via Internet. Le VPN n'est pas utilisé pour accéder aux services d'arrière-plan.

**Serveur Exchange Secure Mail :** définissez la stratégie **Serveur Exchange Secure Mail** sur le nom de domaine complet (FQDN) du serveur de messagerie.

**Services réseau d'arrière-plan :** la stratégie de service réseau d'arrière-plan spécifie la liste des serveurs de messagerie dont l'accès est autorisé via Citrix Gateway. Répertoriez les noms d'hôte

et le numéro de port sous forme de valeur séparée par des virgules. Assurez-vous qu'il n'y a pas d'espaces de début et de fin entre les valeurs. Pour les adresses de serveur de messagerie, incluez : `hostnameFQDN:portnumber`. Par exemple : `mail1.example.com:443,mail2.example.com:443` (pas d'espace entre la virgule).

**Passerelle des services réseau d'arrière-plan :** la stratégie Passerelle des services réseau d'arrière-plan spécifie le boîtier Citrix Gateway que Secure Mail utilise pour se connecter au serveur de messagerie. Pour l'adresse Citrix Gateway, incluez : `citrixgatewayFQDN:portnumber`. Par exemple : `gateway3.example.com:443`.

**Expiration du ticket des services d'arrière-plan :** cette stratégie spécifie la validité d'un ticket de service réseau d'arrière-plan. Lorsque Secure Mail se connecte via Citrix Gateway à un serveur de messagerie, Citrix Endpoint Management émet un jeton utilisé pour se connecter au serveur de messagerie interne. Ce paramètre détermine la durée jusqu'à laquelle Secure Mail peut utiliser ce jeton. Un nouveau jeton pour l'authentification et la connexion au serveur de messagerie n'est pas nécessaire si le jeton est actif. Lorsque la limite de temps expire, les utilisateurs doivent ouvrir une session à nouveau pour générer un nouveau jeton. La valeur par défaut de ce jeton est 168 heures (7 jours).

Pour plus d'informations sur les stratégies d'application MDX pour les services d'arrière-plan, consultez les sections suivantes :

- Stratégies de paramètres de l'application Secure Mail pour Android
- Stratégies de paramètres de l'application Secure Mail pour iOS

La figure suivante montre le flux de communication et les services où ces stratégies sont applicables.

Les figures suivantes présentent les types de connexions Secure Mail à un serveur de messagerie. Une liste des paramètres de stratégie associés s'affiche après chaque figure.

**Connexion directe à un serveur de messagerie :**

Stratégies pour une connexion directe à un serveur de messagerie :

- Accès réseau : **Non restreint**

Si l'accès réseau est illimité, les stratégies suivantes ne s'appliquent pas :

- Services réseau d'arrière-plan
- Expiration du ticket des services d'arrière-plan
- Passerelle des services réseau d'arrière-plan

**Connexion à un serveur de messagerie via STA :**

Stratégies de connexion à un serveur de messagerie via STA :

- Accès réseau : **Tunnélisé vers le réseau interne**
- Services réseau d'arrière-plan : `mail.example.com:443,mail1.example1.com:443`
- Expiration du ticket des services d'arrière-plan : **168**
- Passerelle des services réseau d'arrière-plan : `gateway3.example.com:443`

> **Remarque :**
>
> Citrix vous recommande d'utiliser une connexion STA pour Secure Mail car celle-ci prend en charge les connexions de session de longue durée.

Pour plus d'information sur STA, consultez cet article du Centre de connaissances Citrix.

## Intégration à un serveur Exchange Server ou un serveur IBM Notes Traveler

February 11, 2019

Pour faire en sorte que Secure Mail reste synchronisé avec vos serveurs de messagerie, intégrez Secure Mail à un serveur Exchange Server ou IBM Notes Traveler qui réside sur votre réseau interne ou derrière Citrix Gateway.

- Pour configurer les services d'arrière-plan pour Secure Mail, voir : Services d'arrière-plan pour Secure Mail.
- Pour configurer le serveur IBM Notes Traveler pour Secure Mail, voir : Configuration du serveur IBM Notes Traveler pour Secure Mail.

> **Important :**
>
> Vous ne pouvez pas synchroniser la messagerie à partir de Secure Mail avec IBM Notes Traveler (anciennement IBM Lotus Notes Traveler). Cette fonctionnalité tierce Lotus Notes n'est actuellement pas prise en charge. Par conséquent, lorsque vous supprimez un message de réunion de Secure Mail, ce message n'est pas supprimé sur le serveur IBM Notes Traveler. [CXM-47936]
> Pour en savoir plus sur les limitations avec IBM/Lotus Notes, veuillez consulter ce billet de blog Citrix.

La synchronisation est également disponible pour Secure Notes et Secure Tasks. Veuillez noter cependant que Secure Notes et Secure Tasks ont atteint la fin de leur cycle de vie le 31 décembre 2018. Pour plus d'informations, voir Applications en fin de vie et obsolètes.

- Pour synchroniser Secure Notes pour iOS, intégrez-le à un serveur Exchange.
- Pour synchroniser Secure Notes et Secure Tasks pour Android, utilisez le compte Secure Mail pour Android.

Lorsque vous ajoutez Secure Mail, Secure Notes et Secure Tasks à Citrix Endpoint Management (anciennement XenMobile), configurez les stratégies MDX comme décrit dans Stratégies d'application MDX pour la configuration des services d'arrière-plan.

> **Remarque :**
>
> Secure Mail pour Android et iOS prennent en charge le chemin d'accès complet spécifié pour un serveur Notes Traveler. Par exemple : `https://mail.example.com/traveler/Microsoft-Server-ActiveSync`.
>
> Il n'est plus nécessaire de configurer votre annuaire Domino avec des règles de remplacement de site Web pour le serveur Traveler.

## Configuration du serveur IBM Notes Traveler pour Secure Mail

Dans les environnements IBM Notes, vous devez configurer le serveur IBM Notes Traveler avant de déployer Secure Mail. Cette section présente une illustration de déploiement de cette configuration ainsi que la configuration système requise.

> **Important :**
>
> si votre serveur Notes Traveler utilise SSL 3.0, gardez à l'esprit que SSL 3.0 contient une faille appelée attaque Padding Oracle On Downgraded Legacy Encryption (POODLE), qui est un type d'attaque « man-in-the-middle » qui affecte toute application qui se connecte à un serveur à l'aide de SSL 3.0. Pour résoudre les vulnérabilités introduites par l'attaque POODLE, Secure Mail désactive par défaut les connexions SSL 3.0 et utilise TLS 1.0 pour se connecter au serveur. En conséquence, Secure Mail ne peut pas se connecter à un serveur Notes Traveler qui utilise SSL 3.0. Pour plus de détails sur une solution recommandée, consultez la section Configuration du niveau de sécurité SSL/TLS dans Intégration à un serveur Exchange Server ou un serveur IBM Notes Traveler.

Dans les environnements IBM Notes, vous devez configurer le serveur IBM Notes Traveler avant de déployer Secure Mail.

Le diagramme suivant illustre l'emplacement réseau des serveurs IBM Notes Traveler et un serveur de messagerie IBM Domino dans un déploiement.

## Configuration système requise

### Configuration requise pour le serveur d'infrastructure

- Serveur de messagerie IBM Domino 9.0.1
- IBM Notes Traveler 9.0.1

### Protocoles d'authentification

- Base de données Domino

- Protocole d'authentification Lotus Notes
- Protocole LDAP

**Configuration requise pour les ports**

- Exchange : le port SSL par défaut est 443.
- IBM Notes : SSL est pris en charge sur le port 443. Non-SSL est pris en charge par défaut sur le port 80.

## Configuration du niveau de sécurité SSL/TLS

Citrix a apporté des modifications à Secure Mail pour résoudre les problèmes de vulnérabilité introduits par l'attaque POODLE, comme décrit dans la section Remarque importante qui suit. Si votre serveur Notes Traveler utilise SSL 3.0, il est recommandé, pour activer les connexions, d'utiliser TLS 1.2 sur le serveur IBM Notes Traveler 9.0.

IBM a publié un correctif pour empêcher l'utilisation de SSL 3.0 dans les communications serveur à serveur sécurisées de Notes Traveler. Le correctif, disponible en novembre 2014, est inclus en tant mise à jour provisoire pour les versions suivantes du serveur Notes Traveler : 9.0.1 IF7, 9.0.0.1 IF8 et 8.5.3 Upgrade Pack 2 IF8 (et sera inclus dans les versions ultérieures). Pour de plus amples informations sur le correctif, consultez LO82423: DISABLE SSLV3 FOR TRAVELER SERVER TO SERVER COMMUNICATION.

Une autre solution consiste à modifier la stratégie Niveau de sécurité de la connexion sur **SSLv3 et TLS** lorsque vous ajoutez Secure Mail à Endpoint Management. Pour obtenir plus d'informations sur ce problème, veuillez consulter la section Connexions SSLv3 désactivées par défaut sur Secure Mail 10.0.3.

Le tableau suivant indique les protocoles pris en charge par Secure Mail, par système d'exploitation, en fonction de la valeur de la stratégie Niveau de sécurité de la connexion. Votre serveur de messagerie doit également être en mesure de négocier le protocole.

Le tableau suivant montre les protocoles pris en charge pour Secure Mail lorsque le niveau de sécurité de connexion est SSLv3 et TLS.

| Type de système d'exploitation | SSLv3 | TLS |
|---|---|---|
| iOS 9 et versions ultérieures | Non | Oui |
| Versions antérieures à Android M | Oui | Oui |
| Android M et Android N | Oui | Oui |

| Type de système d'exploitation | SSLv3 | TLS |
|---|---|---|
| Android O | Non | Oui |

Le tableau suivant montre les protocoles pris en charge pour Secure Mail lorsque le niveau de sécurité de connexion est TLS.

| Type de système d'exploitation | SSLv3 | TLS |
|---|---|---|
| iOS 9 et versions ultérieures | Non | Oui |
| Versions antérieures à Android M | Non | Oui |
| Android M et Android N | Non | Oui |
| Android O | Non | Oui |

### Configuration du Serveur Notes Traveler

Les informations suivantes correspondent aux pages du client IBM Domino Administrator.

- **Sécurité :** l'authentification Internet est définie sur Fewer name variations with higher security. Ce paramètre est utilisé pour mapper UID sur AD User ID dans les protocoles d'authentification LDAP.
- **NOTES.INI Settings:** ajoutez **NTS_AS_ENFORCE_POLICY**=**false**. Cela permet aux stratégies Secure Mail d'être gérées par Endpoint Management plutôt que par Traveler. Ce paramètre peut entrer en conflit avec les déploiements clients actuels, mais permet de simplifier la gestion des appareils dans les déploiements Endpoint Management.
- **Protocoles de synchronisation :** SyncML sur IBM Notes et la synchronisation d'appareils mobiles ne sont pas pris en charge par Secure Mail pour le moment. Secure Mail synchronise la messagerie, le calendrier et les contacts via le protocole Microsoft ActiveSync intégré aux serveurs Traveler. Si SyncML est forcé en tant que le protocole principal, Secure Mail ne peut pas se reconnecter au travers de l'infrastructure Traveler.
- **Configuration de l'annuaire Domino - sites Internet Web :** remplacez l'authentification de session pour /traveler pour désactiver l'authentification basée sur les formulaires.

## S/MIME pour Secure Mail

March 12, 2019

Secure Mail prend en charge le protocole S/MIME (Secure/Multipurpose Internet Mail Extensions), qui permet aux utilisateurs de signer et de chiffrer les messages pour plus de sécurité. La signature certifie au destinataire que le message a bien été envoyé par l'expéditeur identifié et non par un imposteur. Le cryptage autorise uniquement les destinataires dotés d'un certificat compatible à ouvrir le message.

Pour plus d'informations sur S/MIME, consultez Microsoft TechNet.

Dans le tableau suivant, un X indique que Secure Mail prend en charge une fonctionnalité S/MIME sur le système d'exploitation d'un appareil.

| Fonctionnalité S/MIME | iOS | Android |
| --- | --- | --- |
| **Intégration d'un fournisseur d'identité numérique :** vous pouvez intégrer Secure Mail avec un fournisseur d'identité numérique tiers pris en charge. Votre hôte de fournisseur d'identité fournit les certificats à une application de fournisseur d'identité sur les appareils utilisateur. Cette application envoie les certificats au coffre partagé Endpoint Management, une zone de stockage sécurisée pour les données applicatives sensibles. Secure Mail obtient des certificats à partir du coffre partagé. Pour de plus amples informations, consultez la section Intégration avec un fournisseur d'identité numérique. | X | |

| Fonctionnalité S/MIME | iOS | Android |
| --- | --- | --- |
| **Prise en charge des informations d'identification dérivées** | Secure Mail prend en charge l'utilisation des informations d'identification dérivées en tant que source de certificat. Pour de plus amples informations, consultez la section Informations d'identification dérivées pour iOS. | |
| **Distribution de certificats par e-mail :** la distribution de certificats e-mail nécessite de créer des modèles de certificat et d'utiliser ces modèles pour demander des certificats utilisateur. Une fois les certificats installés et validés, exportez les certificats utilisateur puis envoyez-les aux utilisateurs par courrier électronique. Les utilisateurs ouvrent ensuite l'e-mail dans Secure Mail et importent les certificats. Pour de plus amples informations, consultez la section Distribution de certificats par e-mail. | X | X |

| Fonctionnalité S/MIME | iOS | Android |
|---|---|---|
| **Importation automatique de certificats monovalents :** Secure Mail détecte si un certificat est uniquement dédié à la signature ou au cryptage, puis importe automatiquement le certificat et notifie l'utilisateur. Si un certificat remplit ces deux rôles, les utilisateurs sont invités à l'importer. | X | |

## Intégration avec un fournisseur d'identité numérique

Le diagramme suivant illustre le chemin emprunté par un certificat de l'hôte fournisseur d'identité numérique jusqu'à Secure Mail. Cela se produit lorsque vous intégrez Secure Mail avec un fournisseur d'identité numérique tiers pris en charge.

Le coffre partagé MDX est une zone de stockage sécurisée pour les données applicatives sensibles telles que les certificats. Seule une application activée par Endpoint Management peut accéder au coffre partagé.

## Conditions préalables

Secure Mail prend en charge l'intégration avec Entrust IdentityGuard.

## Configuration de l'intégration

1. Préparez l'application de fournisseur d'identité et mettez-la à la disposition des utilisateurs :
    - Contactez Entrust afin d'obtenir le fichier .ipa à wrapper.
    - Utilisez l'outil MDX Toolkit pour wrapper l'application.

      Si vous déployez cette application auprès d'utilisateurs qui disposent déjà d'une version de l'application en dehors de l'environnement Endpoint Management, utilisez un ID d'application unique pour cette application. Utilisez le même profil de provisioning pour cette application et Secure Mail.

- Ajoutez l'application à Endpoint Management et publiez-la dans le magasin d'applications Endpoint Management.
- Faites savoir à vos utilisateurs qu'ils doivent installer l'application de fournisseur d'identité depuis Secure Hub. Fournissez des instructions, le cas échéant, sur les étapes de post-installation.

  En fonction de la manière dont vous configurez les stratégies S/MIME pour Secure Mail dans l'étape suivante, Secure Mail peut inviter les utilisateurs à installer des certificats ou activer S/MIME dans les paramètres Secure Mail. Les étapes à suivre pour ces deux procédures sont détaillées dans Activation de S/MIME sur Secure Mail pour iOS.

2. Lorsque vous ajoutez Secure Mail à Endpoint Management, assurez-vous de configurer ces stratégies :
   - Définissez la stratégie Source du certificat S/MIME sur **Coffre partagé**. Ce paramètre signifie que Secure Mail utilise les certificats stockés dans son coffre partagé par votre fournisseur d'identité numérique.
   - Pour activer S/MIME pendant le démarrage initial de Secure Mail, configurez la stratégie Activer S/MIME lors du premier démarrage de Secure Mail. La stratégie détermine si Secure Mail active S/MIME s'il existe des certificats dans le coffre partagé. Si aucun certificat n'est disponible, Secure Mail invite l'utilisateur à importer des certificats. Si cette stratégie n'est pas activée, les utilisateurs peuvent activer S/MIME dans les paramètres Secure Mail. Par défaut, Secure Mail n'active pas S/MIME, ce qui signifie que les utilisateurs doivent l'activer dans les paramètres Secure Mail.

### Utilisation d'informations d'identification dérivées

Plutôt que de passer par l'intégration avec un fournisseur d'identité numérique, vous pouvez autoriser l'utilisation d'informations d'identification dérivées.

Lorsque vous ajoutez Secure Mail à Endpoint Management, configurez la stratégie de source de certificat S/MIME sur **Informations d'identification dérivées**. Pour de plus amples informations, consultez la section Informations d'identification dérivées pour iOS.

### Distribution de certificats par e-mail

Plutôt que de passer par l'intégration avec un fournisseur d'identité numérique ou d'utiliser des informations d'identification dérivées, vous pouvez distribuer des certificats aux utilisateurs par e-mail. Cette option requiert les étapes générales suivantes, détaillées dans cette section.

1. Utilisez le Gestionnaire de serveur pour activer l'inscription Web des services de certificats Microsoft et pour vérifier vos paramètres d'authentification dans IIS.

2. Créez des modèles de certificat pour la signature et le cryptage des messages électroniques. Utilisez ces modèles pour demander des certificats utilisateur.
3. Installez et validez les certificats, exportez-les et envoyez-les aux utilisateurs par e-mail.
4. Les utilisateurs ouvrent l'e-mail dans Secure Mail et importent les certificats. Les certificats sont donc uniquement disponibles pour Secure Mail. Ils ne s'affichent pas dans le profil iOS pour S/MIME.

### Conditions préalables

Les instructions contenues dans cette section sont basées sur les composants suivants :

- XenMobile Server 10 et version ultérieure
- Une version prise en charge de Citrix Gateway, anciennement NetScaler Gateway
- Secure Mail pour iOS (version minimum 10.8.10) ; Secure Mail pour appareils Android (version minimum 10.8.10)
- Microsoft Windows Server 2008 R2 ou version ultérieure avec les services de certificats Microsoft agissant en tant qu'autorité de certification racine (CA)
- Microsoft Exchange :
  - Exchange Server 2016, mise à jour cumulative 4
  - Exchange Server 2013, mise à jour cumulative 15
  - Exchange Server 2010 SP3 Update Rollup 16

Remplissez les conditions préalables suivantes avant de configurer S/MIME :

- Délivrez les certificats racine et intermédiaires aux appareils mobiles, soit manuellement, soit au moyen d'une stratégie d'informations d'identification dans Endpoint Management. Pour plus de détails, consultez la section Stratégie d'informations d'identification.
- Si vous utilisez des certificats de serveur privé pour sécuriser le trafic ActiveSync vers le serveur Exchange, vous devez avoir installé tous les certificats racine et intermédiaires sur les appareils mobiles.

### Activation de l'inscription Web aux Services de certificats Microsoft

1. Accédez à **Outils d'administration** et sélectionnez **Gestionnaire de serveur**.
2. Sous **Services de certificats Active Directory**, vérifiez que la fonction **Inscription de l'autorité de certification via le Web** est installée.
3. Sélectionnez **Ajouter des services de rôle** pour installer l'inscription de l'autorité de certification via le Web, le cas échéant.
4. Cochez la case **Inscription de l'autorité de certification via le Web**, puis cliquez sur **Suivant**.
5. Cliquez sur **Fermer** ou **Terminer** lorsque l'installation est terminée.

### Vérification de vos paramètres d'authentification dans IIS

- Assurez-vous que le site Web d'inscription servant à requérir les certificats utilisateur (par exemple, `https://ad.domain.com/certsrv/`) est sécurisé par un certificat de serveur HTTPS (privé ou public).
- Le site d'inscription Web doit être accessible via HTTPS.

1. Accédez à **Outils d'administration** et sélectionnez **Gestionnaire de serveur**.
2. Dans **Serveur Web (IIS)**, regardez sous **Services de rôle**. Vérifiez que les options Authentification par mappage de certificat client et Authentification par mappage de certificat client IIS sont installées. Si ce n'est pas le cas, installez ces services de rôle.
3. Accédez à **Outils d'administration** et sélectionnez **Gestionnaire des services Internet (IIS)**.
4. Dans le panneau de gauche de la fenêtre **Gestionnaire des services Internet**, sélectionnez le serveur qui exécute l'instance IIS pour inscription Web.
5. Cliquez sur **Authentification**.
6. Assurez-vous que **Authentification du certificat client Active Directory** est **Activé**.
7. Cliquez sur **Sites > Site par défaut de Microsoft Internet Information Services > Liaisons** dans le panneau de droite.
8. Si aucune liaison HTTPS n'existe pas, ajoutez-en une.
9. Accédez à la page d'accueil du site Web par défaut.
10. Cliquez sur **Paramètres SSL** et cliquez sur **Accepter pour les certificats clients**.

### Création de nouveaux modèles de certificats

Pour signer et crypter des messages électroniques, Citrix vous recommande de créer des certificats dans les services de certificats Active Directory de Microsoft. Si vous utilisez le même certificat pour les deux opérations et archivez le certificat de cryptage, vous pouvez récupérer un certificat de signature et autoriser l'emprunt d'identité.

La procédure suivante duplique les modèles de certificat sur le serveur d'autorité de certification (CA) :

- Signature Exchange uniquement (pour la signature)
- Utilisateur Exchange (pour le cryptage)

1. Ouvrez le composant logiciel enfichable Autorité de certification.
2. Développez l'autorité de certification, puis accédez aux **modèles de certificats**.
3. Cliquez avec le bouton droit, puis cliquez sur **Gérer**.
4. Recherchez le modèle Signature Exchange uniquement, cliquez avec le bouton droit sur le modèle, puis cliquez sur **Modèle dupliqué**.
5. Attribuez un nom.

6. Sélectionnez la case **Publier le certificat dans Active Directory**.

   > **Remarque :**
   >
   > Si vous ne sélectionnez pas **Publier le certificat dans Active Directory**, les utilisateurs devront publier les certificats utilisateur (de signature et de cryptage) manuellement. Ils peuvent effectuer ceci via le **client de messagerie Outlook > Centre de gestion de la confidentialité > Sécurité de messagerie électronique > Publier vers la liste d'adresses globale (GAL)**.

7. Cliquez sur l'onglet **Gestion de la demande**, puis entrez les paramètres suivants :

   - **Objectif :** Signature
   - **Taille de clé minimale :** 2048
   - **Case à cocher Autoriser l'exportation de la clé privée :** sélectionnée
   - **Case à cocher Inscrire le sujet sans exiger une entrée utilisateur :** sélectionnée

8. Cliquez sur l'onglet **Sécurité** et sous **Noms de groupes ou d'utilisateurs**, assurez-vous que **Utilisateurs authentifiés** (ou un groupe de sécurité de domaine souhaité) est ajouté. Assurez-vous également que, sous **Autorisations pour utilisateurs authentifiés**, les cases **Lecture et Inscription** sont cochées pour **Autoriser**.

9. Pour tous les autres onglets et paramètres, conservez les paramètres par défaut.

10. Dans les **modèles de certificat**, cliquez sur **Utilisateur Exchange** et répétez les étapes 4 à 9.

    Pour le nouveau modèle Utilisateur Exchange, utilisez les mêmes paramètres par défaut que le modèle d'origine.

11. Cliquez sur l'onglet **Gestion de la demande**, puis entrez les paramètres suivants :

    - **Objectif :** cryptage
    - **Taille de clé minimale :** 2048
    - **Case à cocher Autoriser l'exportation de la clé privée :** sélectionnée
    - **Case à cocher Inscrire le sujet sans exiger une entrée utilisateur :** sélectionnée

12. Lorsque les deux modèles sont créés, veillez à émettre les deux modèles de certificat. Cliquez sur **Nouveau**, puis cliquez sur un **modèle de certificat à émettre**.

### Demande de certificats utilisateur

Cette procédure utilise « utilisateur1 » pour accéder à la page d'inscription Web ; par exemple, `https://ad.domain.com/certsrv/`. La procédure nécessite deux nouveaux certificats utilisateur pour la messagerie sécurisée : un certificat pour la signature et l'autre pour le cryptage. Vous pouvez répéter

la même procédure pour d'autres utilisateurs de domaine qui requièrent l'utilisation de S/MIME via Secure Mail.

Une inscription manuelle est utilisée via le site Web d'inscription (par exemple, `https://ad.domain.com/certsrv/`) sur Microsoft Certificate Services pour générer les certificats utilisateur de signature et de cryptage. Une autre solution consiste à configurer l'inscription automatique au moyen d'une stratégie de groupe pour le groupe d'utilisateurs qui souhaiterait utiliser cette fonction.

1. Sur un ordinateur Windows, ouvrez Internet Explorer, puis accédez au site Web d'inscription pour demander un nouveau certificat utilisateur.

   > **Remarque :**
   >
   > veillez à ouvrir une session avec le bon compte utilisateur de domaine pour la demande de certificat.

2. Une fois connecté, cliquez sur **Demander un certificat**.
3. Cliquez sur **Demande de certificat avancée**.
4. Cliquez sur **Créer et soumettre une demande de requête auprès de cette Autorité de certification**.
5. Générez le certificat utilisateur pour la signature. Sélectionnez le nom de modèle approprié et entrez vos paramètres utilisateur, puis sélectionnez **PKCS10** à côté de **Format de la demande**.

   La demande a été envoyée.

6. Cliquez sur **Installer ce certificat**.
7. Vérifiez que le certificat est correctement installé.
8. Répétez la même procédure, mais cette fois pour le cryptage des messages électroniques. Avec le même utilisateur connecté au site Web d'inscription, cliquez sur le lien Page d'accueil pour demander un nouveau certificat.
9. Sélectionnez le nouveau modèle pour le cryptage, puis entrez les mêmes paramètres utilisateur entrés à l'étape 5.
10. Assurez-vous d'avoir installé le certificat avec succès et répétez la même procédure pour générer une paire de certificats utilisateur pour un autre utilisateur de domaine. Cet exemple suit la même procédure et génère une paire de certificats pour l'« Utilisateur2 ».

    > **Remarque :**
    >
    > Cette procédure utilise le même ordinateur Windows pour demander la seconde paire de certificats pour l'« Utilisateur2 ».

### Validation des certificats publiés

1. Pour vous assurer que les certificats sont correctement installés dans le profil de l'utilisateur de domaine, allez sur **Utilisateurs et ordinateurs Active Directory > Afficher > Fonctionnalités avancées**.
2. Accédez aux propriétés de l'utilisateur (Utilisateur1 pour cet exemple), puis cliquez sur l'onglet des **certificats publiés**. Assurez-vous que les deux certificats sont disponibles. Vous pouvez également vérifier que chaque certificat est dédié à un usage spécifique.

   Ce diagramme illustre un certificat réservé au cryptage des messages électroniques.

   Ce diagramme illustre un certificat réservé à la signature des messages électroniques.

   Assurez-vous que le bon certificat de cryptage est attribué à l'utilisateur. Vous pouvez vérifier ces informations dans **Utilisateurs et ordinateurs Active Directory > propriétés utilisateur**.

   Secure Mail opère en vérifiant l'attribut userCertificate de l'objet utilisateur au moyen de requêtes LDAP. Vous pouvez lire cette valeur dans l'onglet **Éditeur d'attributs**. Si ce champ est vide ou contient un certificat utilisateur de cryptage erroné, Secure Mail ne pourra pas crypter (ni décrypter) les messages.

### Exportation des certificats utilisateur

Cette procédure exporte les deux paires de certificats « Utilisateur1 » et « Utilisateur2 » au format .PFX (PKCS#12) avec la clé privée. Une fois exportés, les certificats sont envoyés par courrier électronique à l'utilisateur à l'aide d'Outlook Web Access (OWA).

1. Ouvrez la console MMC et accédez au composant logiciel enfichable **Certificats - Utilisateur actuel**. Les deux paires de certificats pour les « Utilisateur1 » et « Utilisateur2 » s'affichent.
2. Cliquez avec le bouton droit sur le certificat, puis cliquez sur **Toutes les tâches > Exporter**.
3. Exportez la clé privée en sélectionnant **Oui, exporter la clé privée**.
4. Sélectionnez les cases **Si possible inclure tous les certificats dans le chemin d'accès de certification si possible** et **Exporter toutes les propriétés étendues**.
5. Lorsque vous exportez le premier certificat, répétez la même procédure pour les certificats utilisateur restants.

   > **Remarque :**
   >
   > Identifiez clairement les certificats de signature et de cryptage. Dans l'exemple, les certificats sont nommés « userX-sign.pfx » et « userX-enc.pfx ».

### Envoi des certificats par courrier électronique

Lorsque tous les certificats sont exportés au format PFX, vous pouvez utiliser Outlook Web Access (OWA) pour les envoyer par courrier électronique. Le nom utilisé pour la connexion dans cet exemple est Utilisateur1, le courrier électronique envoyé contient les deux certificats.

Répétez la même procédure pour l'Utilisateur2 ou d'autres utilisateurs de votre domaine.

### Activation de S/MIME sur Secure Mail pour iOS et Android

Une fois le message reçu, l'étape suivante consiste à ouvrir le message avec Secure Mail puis à activer S/MIME avec les certificats appropriés pour la signature et le cryptage.

#### Pour activer S/MIME avec des certificats de signature et de cryptage individuels

1. Ouvrez Secure Mail, accédez à l'e-mail contenant les certificats S/MIME.
2. Touchez le certificat de signature à télécharger et importer.
3. Tapez le mot de passe affecté à la clé privée lorsque le certificat de signature a été exporté depuis le serveur.

   Votre certificat a été importé.
4. Touchez **Activer la signature**.
5. Vous pouvez aussi accéder à **Paramètres (ou Réglages)** > et **S/MIME** et toucher S/MIME pour activer le certificat de signature.
6. Dans l'écran **Signature**, vérifiez que le bon certificat de signature a été importé.
7. Revenez à l'e-mail et touchez le certificat de cryptage à télécharger et à importer.
8. Tapez le mot de passe affecté à la clé privée lorsque le certificat de cryptage a été exporté depuis le serveur.

   Votre certificat a été importé.
9. Touchez **Activer le cryptage**.
10. Vous pouvez aussi accéder à **Paramètres (ou Réglages)** > et **S/MIME** et toucher S/MIME pour activer **Crypter par défaut**.
11. Dans l'écran **Cryptage**, vérifiez que le bon certificat de cryptage a été importé.

> **Remarque :**
>
> a) Si un e-mail est signé numériquement avec S/MIME, qu'il possède des pièces jointes, et que le destinataire n'a pas activé S/MIME, les pièces jointes ne seront pas reçues. Ce

comportement est une limitation d'ActiveSync. Pour recevoir des messages S/MIME, activez S/MIME dans les paramètres de Secure Mail.

b) L'option **Crypter par défaut** vous permet de minimiser les étapes requises pour crypter votre e-mail.
Si cette fonctionnalité est activée, votre e-mail sera crypté lors de sa rédaction.
Si cette fonctionnalité est désactivée, votre e-mail ne sera pas crypté lors de sa rédaction et vous devez taper sur l'icône **Verrouiller** pour le crypter.

**Pour activer S/MIME avec un seul certificat de signature et de cryptage**

1. Ouvrez Secure Mail, accédez à l'e-mail contenant le certificat S/MIME.
2. Touchez le certificat S/MIME à télécharger et importer.
3. Tapez le mot de passe affecté à la clé privée lorsque le certificat a été exporté depuis le serveur.
4. Dans les options de certificat qui apparaissent, touchez l'option appropriée pour importer un certificat de signature ou un certificat de cryptage.
   Appuyez sur **Ouvrir certificat** pour afficher les détails du certificat.

   Votre certificat a été importé.

   Vous pouvez afficher les certificats importés en accédant à **Paramètres (ou Réglages) > S/MIME**

## Test de S/MIME sur iOS et Android

Une fois que vous avez exécuté les étapes répertoriées dans la section précédente, votre destinataire peut lire votre e-mail signé et crypté.

L'image suivante montre un exemple de message crypté lu par le destinataire.

La figure suivante montre un exemple de vérification du certificat de signature approuvé.

Secure Mail recherche dans le domaine Active Directory les certificats de cryptage public des destinataires. Si un utilisateur envoie un message crypté à un destinataire qui ne dispose pas d'une clé de cryptage publique valide, le message n'est pas crypté. Dans un message de groupe, il suffit qu'un seul destinataire ne dispose pas d'une clé valide pour que le message envoyé à tous les destinataires ne soit pas crypté.

## Configuration de sources de certificat public

Pour utiliser les certificats publics S/MIME, configurez la source du certificat public S/MIME, l'adresse du serveur LDAP, le nom unique de base LDAP et les stratégies Accès anonyme à LDAP.

En plus des stratégies applicatives, procédez comme suit.

- Si les serveurs LDAP sont publics, assurez-vous que le trafic est directement acheminé aux serveurs LDAP. Pour ce faire, configurez la stratégie réseau de Secure Mail sur **Tunnélisé vers le réseau interne** et configurez le split DNS pour Citrix ADC.
- Si les serveurs LDAP sont hébergés sur un réseau interne, procédez comme suit :
  - Pour iOS, assurez-vous de ne pas configurer la stratégie Passerelle des services réseau d'arrière-plan. Si vous configurez la stratégie, les utilisateurs reçoivent des invites d'authentification fréquentes.
  - Pour Android, assurez-vous d'ajouter l'**URL du serveur LDAP** dans la liste pour la stratégie Passerelle des services réseau d'arrière-plan.

## Authentification unique (SSO) pour Secure Mail

January 14, 2019

Vous pouvez configurer Endpoint Management de manière à inscrire automatiquement les utilisateurs auprès de Secure Mail lorsqu'ils s'inscrivent dans Secure Hub. Les utilisateurs n'ont pas à entrer d'informations supplémentaires ou à effectuer des étapes supplémentaires pour s'inscrire dans Secure Mail. Pour les utilisateurs qui s'inscrivent auprès de Secure Hub à l'aide d'informations d'identification de messagerie, cette fonctionnalité nécessite que la détection automatique soit activée. Si la découverte automatique n'est pas activée, vous pouvez activer cette fonctionnalité pour les méthodes d'inscription suivantes :

- L'adresse de Endpoint Management est transmise à Secure Mail depuis Secure Hub.
- Les utilisateurs entrent l'adresse de Endpoint Management lorsqu'ils s'inscrivent auprès de Secure Hub.

### Pour activer l'inscription automatique dans Secure Mail

1. Définissez ces propriétés du client Endpoint Management sur **vrai** :
   - ENABLE_PASSCODE_AUTH
   - ENABLE_PASSWORD_CACHING
   - ENABLE_CREDENTIAL_STORE
2. Ajoutez cette propriété du client Endpoint Management :

   Nom d'affichage : SEND_LDAP_ATTRIBUTES

   Value:userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}
3. Ajoutez cette propriété Endpoint Management :

   MAM_MACRO_SUPPORT définie sur **true**

4. Configurez ces propriétés Secure Mail :
    - Définissez Mécanisme d'authentification initial sur **Adresse e-mail de l'utilisateur**.
    - Définissez Informations d'identification d'authentification initiales sur **userPrincipalName**.
5. Configurez le service de découverte automatique basé sur les e-mails pour la boîte aux lettres Exchange Server de l'utilisateur. Pour obtenir de l'aide, contactez votre administrateur Microsoft Exchange. Cet article suppose que vous configurez le service de découverte automatique en interrogeant DNS pour un enregistrement SRV.

### Pour configurer la stratégie d'application Secure Mail

Téléchargez l'application Secure Mail sur Endpoint Management. Téléchargez le fichier .mdx associé à la version correcte de l'application Secure Mail. Ensuite, configurez les paramètres de l'application Secure Mail suivants :

1. Sous Mécanisme d'authentification initial, cliquez sur **Adresse e-mail de l'utilisateur**.
2. Sous **Informations d'identification d'authentification initiales**, cliquez sur **userPrincipalName** ou **sAMAccountName**. Votre sélection est basée sur le type d'authentification configuré sur le serveur de messagerie Exchange de l'utilisateur.
3. Laissez les champs du domaine d'utilisateur Serveur Exchange Secure Mail et Secure Mail vides.
4. Configurez les autres stratégies de l'application Secure Mail selon les besoins et effectuez les attributions de groupe de mise à disposition nécessaires.

### Expérience utilisateur à authentification unique (SSO) pour Secure Mail de bout en bout avec approvisionnement automatique

Assurez-vous de remplir les conditions préalables suivantes.

1. Installez Secure Hub à partir de l'App Store d'Apple (iOS) ou du Google Play Store (Android).
2. Ouvrez Secure Hub et entrez une adresse e-mail et un mot de passe pour vous inscrire à Endpoint Management.
3. Installez Secure Mail à partir de l'App Store d'Apple (iOS) ou du Google Play Store (Android).
4. Ouvrez Secure Mail et touchez **OK**. Cette étape permet à Secure Hub de gérer Secure Mail. À l'ouverture, Secure Mail est automatiquement configuré.

Le serveur Exchange correspondant à la base de données de boîtes aux lettres de l'utilisateur est obtenu à partir du service de découverte automatique que vous avez configuré. La demande d'enregistrement SRV DNS utilise l'adresse e-mail de l'utilisateur extraite de Secure Hub.

Tous les détails requis pour la configuration du compte, tels que l'adresse e-mail, userPrincipalName/sAMAccountName et le mot de passe sont récupérés à partir de Secure Hub.

Lorsque le compte est configuré, les utilisateurs peuvent afficher les détails sur l'appareil à partir de **Secure Mail** > **Paramètres** > **Compte**.

### Résoudre les problèmes

Si des problèmes se produisent avec la configuration SSO, vous pouvez essayer les étapes suivantes.

1. Assurez-vous que la version de XenMobile Server est 10.5 ou une version ultérieure.
2. Assurez-vous que Endpoint Management est configuré pour le service de découverte automatique et que l'inscription de l'utilisateur est configurée pour être utilisée avec une adresse e-mail.
3. Assurez-vous que le domaine Exchange Server est configuré avec la découverte automatique. Assurez-vous que la demande d'enregistrement SRV renvoie les détails du serveur de messagerie attendu pour les clients de messagerie ActiveSync.
4. En cas de problème avec cette fonctionnalité, collectez les informations suivantes et contactez le support technique de Citrix :
    - Téléchargez les journaux de diagnostic Endpoint Management.
    - Collectez les journaux de diagnostic de Secure Mail avec le niveau de journalisation le plus élevé.
    - Collectez les journaux IIS à partir du répertoire C:\inetpub\logs\LogFiles\W3SVC1 à partir du serveur Exchange hébergeant le service de découverte automatique. Pour plus de détails sur le Autodiscovery Service de Microsoft, consultez Autodiscover service in Exchange Server.

## Considérations de sécurité

February 19, 2019

Cet article traite des considérations de sécurité de Secure Mail et des paramètres spécifiques que vous pouvez activer pour accroître la sécurité des données.

### Prise en charge de la protection des droits de messagerie IRM et AIP de Microsoft

Secure Mail pour Android et iOS prennent en charge les messages protégés par la gestion des droits relatifs à l'information (IRM) de Microsoft et la solution Azure Information Protection (AIP). Cette prise en charge est soumise à la stratégie IRM configurée sur Citrix Endpoint Management.

Cette fonctionnalité permet aux organisations qui utilisent IRM d'appliquer une protection au contenu de la messagerie. La fonctionnalité permet également aux utilisateurs d'appareils mobiles de créer et de consommer du contenu protégé par des droits. La prise en charge IRM est **désactivée** par défaut. Pour l'activer, définissez la stratégie Gestion des droits relatifs à l'information sur **Activé**.

**Pour activer la gestion des droits relatifs à l'information dans Secure Mail**

1. Connectez-vous à Endpoint Management, accédez à **Configurer** > **Applications**, puis cliquez sur **Ajouter**.
2. Dans l'écran **Ajouter une application**, cliquez sur **MDX**.
3. Dans l'écran **Informations sur l'application** entrez les détails de l'application et cliquez sur **Suivant**.
4. Sélectionnez et téléchargez le fichier .mdx correspondant au système d'exploitation de votre appareil.
5. Activez la gestion des droits relatifs à l'information sous **Paramètres application**.

> Remarque :
>
> Activez la gestion des droits relatifs à l'information pour iOS et Android.

**Lorsque vous recevez un e-mail protégé par des droits**

Lorsque les utilisateurs reçoivent un e-mail contenant du contenu protégé, l'écran suivant s'affiche :

Pour afficher des détails sur les droits auxquels l'utilisateur a droit, appuyez sur **Details**.

**Lorsque vous composez un e-mail protégé par des droits**

Lorsque les utilisateurs composent un e-mail, ils peuvent définir des profils de restriction pour activer la protection de la messagerie.

**Pour définir des restrictions à votre e-mail :**

1. Connectez-vous à Secure Mail et appuyez sur l'icône **Composer**.
2. Dans l'écran de composition, appuyez sur l'icône de **restriction d'e-mail**.
3. Dans l'écran **Profils de restriction**, appuyez sur les restrictions à appliquer à l'e-mail, puis cliquez sur Précédent.

   Les restrictions appliquées apparaissent sous le champ Objet.

Certaines organisations peuvent nécessiter un strict respect de la stratégie IRM. Les utilisateurs ayant accès à Secure Mail peuvent essayer de contourner la stratégie IRM en altérant Secure Mail, le système d'exploitation ou même la plate-forme matérielle.

Bien que Endpoint Management puisse détecter certaines attaques, les mesures de prévention suivantes peuvent accroître la sécurité :

- Consultez le guide de sécurité fourni par le fabricant de l'appareil.
- Configurez les appareils en conséquence, à l'aide des fonctions de Endpoint Management ou d'autres fonctions.
- Conseillez vos utilisateurs dans le cadre de l'utilisation appropriée des fonctionnalités IRM, y compris Secure Mail.
- Déployez des logiciels de sécurité tiers conçus pour résister à ce type d'attaque.

### Classifications de sécurité de la messagerie

Secure Mail pour iOS et Android prend en charge les marquages de classification de messagerie, ce qui permet aux utilisateurs de spécifier des marqueurs SEC (sécurité) et DLM (dissemination limiting markers) lors de l'envoi d'e-mails. SEC comprend les marquages suivants : Protected, Confidential et Secret. DLM comprend les marquages suivants : Sensitive, Legal ou Personal. Lors de la composition d'un e-mail, un utilisateur Secure Mail peut sélectionner un marquage pour indiquer le niveau de classification de l'e-mail, comme indiqué dans les images suivantes.

Les destinataires peuvent afficher le marquage de classification dans l'objet de l'e-mail. Par exemple :

- Objet : Planification [SEC = PROTECTED, DLM = Sensitive]
- Objet : Planification [SEC = PROTECTED, DLM = Sensitive]
- Objet : Planification [SEC = UNCLASSIFIED]

Les en-têtes d'e-mail incluent les marquages de classification comme une extension d'en-tête de message Internet, affiché en gras dans cet exemple :

Date : Ven, 01 Mai 2015 12:34:50 +530

Objet : Planification [SEC = PROTECTED, DLM = Sensitive]

Priorité : normale

X-Priority : normale **X-Protective-Marking: VER-2012.3, NS=gov.au,SEC = PROTECTED, DLM = Sensitive,ORIGIN=operations@example.com**

De : **operations@example.com**

À : Équipe **<mylist@example.com>**

Version MIME : 1.0 Type de contenu : `multipart/alternative;boundary="_com.example.email_6428E5E4-9DB3-4133-9F48-155913E39A980"`

Secure Mail affiche uniquement les marquages de classification. L'application ne prend aucune action basée sur ces marquages.

Lorsqu'un utilisateur répond ou transfère un e-mail contenant des marquages de classification, les valeurs SEC et DLM utilisées par défaut sont les marquages de l'e-mail d'origine. L'utilisateur peut choisir un autre marquage. Secure Mail ne valide pas de telles modifications en relation avec le message d'origine.

Vous configurez les marquages de classification de messagerie par le biais des stratégies MDX suivantes.

- **Classification de la messagerie :** si ce paramètre est défini sur **Activé**, Secure Mail prend en charge les marquages de classification de messagerie pour SEC et DLM. Les marquages de classification apparaissent dans les en-têtes d'e-mail en tant que valeurs « X-Protective-Marking ». Veillez à configurer les stratégies de classification de messagerie associées. La valeur par défaut est **Désactivé**.
- **Espace de noms de classification de la messagerie :** spécifie l'espace de noms de la classification requis dans l'en-tête de l'e-mail par la norme de classification utilisée. Par exemple, l'espace de noms « gov.au » apparaît dans l'en-tête comme « NS=gov.au ». La valeur par défaut est vide.
- **Version de classification de la messagerie :** spécifie la version de la classification requise dans l'en-tête de l'e-mail par la norme de classification utilisée. Par exemple, la version « 2012.3 » apparaît dans l'en-tête comme « VER=2012.3 ». La valeur par défaut est vide.
- **Classification de messagerie par défaut :** spécifie le marquage de protection que Secure Mail applique à un e-mail si un utilisateur ne choisit pas un marquage. Cette valeur doit figurer dans la liste de la stratégie Marquages de classification de la messagerie. La valeur par défaut est **UNOFFICIAL**.
- **Marquages de classification de la messagerie :** spécifie les marquages classification à mettre à la disposition des utilisateurs. Si la liste est vide, Secure Mail ne comprend pas de liste des marquages de protection. La liste des marquages contient des paires de valeurs qui sont séparées par des points-virgules. Chaque paire comprend la valeur de liste qui apparaît dans Secure Mail et la valeur de marquage qui correspond au texte ajouté à l'objet et l'en-tête de l'e-mail dans Secure Mail. Par exemple, dans la paire de marquage « UNOFFICIAL SEC=UNOFFICIAL; », la valeur de liste est « UNOFFICIAL » et la valeur de marquage est « SEC=UNOFFICIAL ».

La valeur par défaut est une liste des marquages de classification que vous pouvez modifier. Les marquages suivants sont fournis avec Secure Mail.

- UNOFFICIAL,SEC=UNOFFICIAL

- UNCLASSIFIED,SEC=UNCLASSIFIED
- For Official Use Only,DLM=For-Official-Use-Only
- Sensitive,DLM=Sensitive
- Sensitive:Legal,DLM=Sensitive:Legal
- Sensitive:Personal,DLM=Sensitive:Personal
- PROTECTED,SEC=PROTECTED
- PROTECTED+Sensitive,SEC=PROTECTED
- PROTECTED+Sensitive:Legal,SEC=PROTECTED DLM=Sensitive:Legal
- PROTECTED+Sensitive:Personal,SEC=PROTECTED DLM=Sensitive:Personal
- PROTECTED+Sensitive:Cabinet,SEC=PROTECTED,DLM=Sensitive:Cabinet
- CONFIDENTIAL,SEC=CONFIDENTIAL
- CONFIDENTIAL+Sensitive,SEC=CONFIDENTIAL,DLM=Sensitive
- CONFIDENTIAL+Sensitive:Legal,SEC=CONFIDENTIAL DLM=Sensitive:Legal
- CONFIDENTIAL+Sensitive:Personal,SEC=CONFIDENTIAL,DLM=Sensitive:Personal
- CONFIDENTIAL+Sensitive:Cabinet,SEC=CONFIDENTIAL DLM=Sensitive:Cabinet
- SECRET,SEC=SECRET
- SECRET+Sensitive,SEC=SECRET,DLM=Sensitive
- SECRET+Sensitive:Legal,SEC=SECRET,DLM=Sensitive:Legal
- SECRET+Sensitive:Personal,SEC=SECRET,DLM=Sensitive:Personal
- SECRET+Sensitive:Cabinet,SEC=SECRET,DLM=Sensitive:Cabinet
- TOP-SECRET,SEC=TOP-SECRET
- TOP-SECRET+Sensitive,SEC=TOP-SECRET,DLM=Sensitive
- TOP-SECRET+Sensitive:Legal,SEC=TOP-SECRET DLM=Sensitive:Legal
- TOP-SECRET+Sensitive:Personal,SEC=TOP-SECRET DLM=Sensitive:Personal
- TOP-SECRET+Sensitive:Cabinet,SEC=TOP-SECRET DLM=Sensitive:Cabinet

### Protection des données iOS

Les entreprises qui doivent satisfaire aux exigences du ASD (Australian Signals Directorate) en matière de protection des données peuvent utiliser la nouvelle stratégie **Activer la protection des données iOS** pour Secure Mail et Secure Web. Par défaut, les stratégies sont définies sur **Désactivé**.

Lorsque la stratégie **Activer la protection des données iOS** est définie sur **Activé** pour Secure Web, Secure Web utilise un niveau de protection de classe A pour tous les fichiers du sandbox. Pour obtenir des informations détaillées sur la protection de données Secure Mail, consultez la section Australian Signals Directorate Data Protection. Si vous activez cette stratégie, la classe de protection des données la plus élevée est utilisée. Il n'est donc pas nécessaire de spécifier également la stratégie **Classe de protection des données minimum**.

**Pour modifier la stratégie Activer la protection des données iOS**

1. Utilisez la console Endpoint Management pour charger les fichiers MDX Secure Web et Secure Mail sur Endpoint Management : pour une nouvelle application, accédez à **Configurer > Applications > Ajouter**, puis cliquez sur **MDX**. Pour une mise à niveau, consultez la section Mettre à niveau les applications MDX ou d'entreprise.
2. Pour Secure Mail, accédez aux paramètres d'**application**, localisez la stratégie **Activer la protection des données iOS** et définissez-la sur **Activé**. Les appareils exécutant des systèmes d'exploitation plus anciens ne sont pas affectés lorsque cette stratégie est activée.
3. Pour Secure Web, accédez au Paramètres d'**application**, localisez la stratégie **Activer la protection des données iOS** et définissez-la sur **Activé**. Les appareils exécutant des systèmes d'exploitation plus anciens ne sont pas affectés lorsque cette stratégie est activée.
4. Configurez les stratégies applicatives et enregistrez vos paramètres pour déployer l'application sur le magasin d'applications Endpoint Management.

## Australian Signals Directorate Data Protection

Secure Mail prend en charge la protection des données du ASD (Australian Signals Directorate) pour les entreprises qui doivent satisfaire aux exigences de sécurité informatique du ASD. Par défaut, la stratégie Activer la protection des données iOS est définie sur **Désactivé**, et Secure Mail offre une protection des données de classe C ou utilise la protection des données définie dans le profil de provisioning.

Si cette stratégie est définie sur **Activé**, Secure Mail spécifie le niveau de protection lors de la création et de l'ouverture des fichiers dans le sandbox des applications. Secure Mail définit la protection des données de classe A sur :

- Les éléments de la Boîte d'envoi
- Les photos provenant de l'appareil photo ou de l'application pellicule
- Les images collées à partir d'autres applications
- Les pièces jointes téléchargées

Secure Mail définit la protection des données de classe B sur :

- Les messages stockés
- Les éléments de calendrier
- Contacts
- Les fichiers de stratégie ActiveSync

La protection de classe B permet la synchronisation d'un appareil verrouillé et autorise les téléchargements si un appareil est verrouillé après le démarrage du téléchargement.

Lorsque la protection des données est activée, les éléments de la boîte d'envoi en file d'attente ne sont pas envoyés lorsqu'un appareil est verrouillé car les fichiers ne peuvent pas être ouverts. Si l'appareil ferme puis redémarre Secure Mail alors qu'un appareil est verrouillé, Secure Mail ne peut pas se synchroniser tant que l'appareil n'est pas déverrouillé et que Secure Mail n'a pas redémarré.

Citrix vous recommande, si vous activez cette stratégie, d'activer la journalisation Secure Mail uniquement en cas de nécessité pour éviter la création de fichiers journaux avec la protection des données de classe C.

## Fonctionnalités Android

March 7, 2019

Cet article décrit les fonctionnalités Android prises en charge sur Secure Mail.

### Affichage des pièces jointes

Dans Secure Mail pour Android, l'affichage des pièces jointes au courrier et au calendrier est facile. La pièce jointe s'ouvre directement dans l'application ou une liste des applications prises en charge apparaît. Vous pouvez sélectionner l'application requise pour afficher la pièce jointe.

Secure Mail prend en charge l'affichage de fichiers .txt, word, audio, vidéo, html, .zip, images, .eml et .vcf contact.

#### Conditions préalables

Assurez-vous qu'un administrateur configure les stratégies MDX suivantes dans la console Citrix Endpoint Management :

- Stratégie Échange de documents (Ouvrir dans) définie sur **Non restreint**.
- Stratégie Autoriser les documents hors connexion définie sur **Illimité**.

Pour de plus amples informations sur ces stratégies, veuillez consulter la section Interaction des applications.

#### Actions lors de l'affichage des pièces jointes

Vous pouvez effectuer les opérations suivantes lorsque vous affichez les pièces jointes :

- Sélectionner un message existant dans vos boîtes aux lettres auquel joindre le fichier
- Créer un message auquel joindre le fichier.
- Enregistrer une pièce jointe pour un accès hors connexion.

- Supprimer la pièce jointe des fichiers hors connexion.
- Ouvrir une pièce jointe à l'aide d'une autre application lorsque vous y êtes invité.
- Afficher l'e-mail source ou l'événement de calendrier de la pièce jointe

Vous pouvez prévisualiser les pièces jointes lors des actions suivantes :

- Affichage d'un message
- Composition d'un nouveau message
- Transfert d'un message.

Vous pouvez également prévisualiser les pièces jointes à ces emplacements :

- Dossier **Pièces jointes** .
- Événements de calendrier.

#### Joindre des fichiers à un e-mail existant ou à un nouvel e-mail

Vous pouvez joindre des fichiers à un e-mail existant ou créer un e-mail pour joindre des fichiers.

1. Appuyez sur le dossier **Pièces jointes**, appuyez longuement pour sélectionner plusieurs pièces jointes, ou appuyez simplement sur une seule pièce jointe pour la sélectionner.

   .

2. Touchez l'icône **Joindre** sur l'écran. La boîte aux lettres apparaît.
3. Vous pouvez effectuer l'une des opérations suivantes :
   - Pour joindre le fichier à un e-mail existant, sélectionnez un message existant.
   - Pour joindre le fichier à un nouvel e-mail, appuyez sur **Nouveau message**.

#### Pour enregistrer la pièce jointe pour un accès hors connexion

1. Ouvrez la pièce jointe.
2. Touchez l'icône **Plus** en haut à droite de la page, puis **Accès hors connexion**.

#### Pour supprimer la pièce jointe des fichiers hors connexion

1. Ouvrez la pièce jointe.
2. Touchez l'icône **Plus** en haut à droite de la page, puis **Suppr. fichiers hors connexion**.

**Pour ouvrir la pièce jointe à l'aide d'une autre application**

1. Ouvrez la pièce jointe.
2. Touchez l'icône **Plus** en haut à droite de la page, puis **Ouvrir avec**.
3. Touchez l'option avec laquelle vous souhaitez ouvrir la pièce jointe.
4. Vous pouvez également faire glisser votre doigt vers la gauche pour afficher la liste des actions qui peuvent être utilisées pour afficher ou ouvrir une pièce jointe.

**Pour afficher l'e-mail source ou l'événement de calendrier de la pièce jointe**

1. Touchez l'icône **Pièces jointes** en bas à droite de votre écran.
2. Touchez la pièce jointe, puis l'icône **Plus** située dans le coin supérieur droit de l'écran.
3. Appuyez sur **Afficher e-mail d'origine** ou **Afficher événement d'origine** pour afficher la source d'un e-mail ou d'un événement de calendrier.

## Imprimer des e-mails et des événements de calendrier

Dans Secure Mail pour Android, vous pouvez imprimer des e-mails et des événements de calendrier à partir de votre appareil Android. Cette fonctionnalité d'impression utilise Android Print Framework.

**Conditions préalables**

- Assurez-vous qu'un administrateur a défini la stratégie **Bloquer l'impression** sur **Désactivé** dans la console Citrix Endpoint Management. Pour plus d'informations sur cette stratégie pour Android, voir la stratégie Bloquer l'impression.
- Si un e-mail est protégé par IRM, assurez-vous d'activer l'option **Autoriser les visionneuses à imprimer** dans l'e-mail.

Vous ne pouvez pas imprimer un e-mail ou un événement de calendrier si ces stratégies sont définies de manière inappropriée.

> **Remarque :**
>
> cette capacité d'impression présente les limitations connues suivantes :
>
> - Les images en ligne ne s'impriment que si vous avez téléchargé des images en appuyant sur **Afficher les images**. Si vous ne tapez pas sur **Afficher les images**, seuls les espaces réservés aux images sont imprimés.
> - Dans Secure Mail, les e-mails volumineux sont tronqués. Avant d'imprimer, appuyez sur

> **Télécharger le message complet** pour imprimer l'e-mail complet. Si le message complet ne se télécharge pas, un e-mail tronqué est imprimé.
> • Aucune métadonnée provenant d'un e-mail ou d'un événement n'est ajoutée lors de l'impression de ces éléments.

**Pour imprimer un e-mail**

1. Ouvrez l'e-mail que vous souhaitez imprimer.
2. Touchez l'icône Plus en haut à gauche de l'écran. Les options suivantes s'affichent :
    - Déplacer
    - Imprimer

> **Remarque :**
>
> Sur les tablettes, vous pouvez directement utiliser l'icône d'impression en haut à gauche de l'écran pour imprimer un e-mail.

1. Appuyez sur **Print**. Un aperçu de votre e-mail apparaît.
2. Appuyez sur la liste pour afficher les options suivantes :
    - Save as PDF (Enregistrer au format PDF)
    - All printers (Toutes les imprimantes)
3. Appuyez sur **Save as PDF** pour enregistrer votre e-mail au format PDF.
4. Appuyez sur **All printers**. Installez l'imprimante selon vos besoins.
5. Une fois l'imprimante installée, appuyez sur **Select Printer** pour sélectionner une imprimante. L'écran **Printer** s'affiche.

    > **Remarque :**
    >
    > Les options d'impression varient en fonction de l'imprimante sélectionnée. L'image suivante provient d'une imprimante Canon E480. Elle est utilisée à des fins de représentation uniquement.

6. Sélectionnez l'imprimante sur laquelle vous souhaitez imprimer. Utilisez les options d'impression suivantes :
    - Entrez manuellement le nombre de copies que vous souhaitez imprimer.
    - Sélectionnez le format de papier dans la liste.
    - Sélectionnez la couleur dans la liste.
    - Choisissez l'orientation de la page selon vos besoins.
    - Sélectionnez une page ou une plage de pages et entrez manuellement la plage de pages.
7. Après avoir configuré les options d'impression, appuyez sur l'icône Imprimer sur l'écran.

**Pour imprimer une image en ligne**

- Appuyez sur **Show pictures** dans l'e-mail et suivez les instructions décrites dans la section précedente Pour imprimer un e-mail.

**Pour imprimer un événement de calendrier**

1. Accédez au calendrier et appuyez sur un événement.
2. Touchez l'icône d'impression et suivez les instructions décrites dans la section précédente Pour imprimer un e-mail.

## Signaler des e-mails de phishing avec des en-têtes ActiveSync

Dans Secure Mail pour Android, lorsqu'un utilisateur signale un courrier de phishing, un fichier EML est généré en tant que pièce jointe correspondant à ce courrier. Les administrateurs reçoivent ce courrier et peuvent afficher les en-têtes ActiveSync associés au courrier signalé.

Pour activer cette fonctionnalité, un administrateur doit configurer la stratégie Signaler les adresses e-mail de phishing et définir Mécanisme de signalisation de phishing sur **Signaler via pièce jointe** dans la console Citrix Endpoint Management. Pour plus de détails, consultez la section Signaler les e-mails de phishing (en tant que pièce jointe).

## Notifications de sous-dossier

Dans Secure Mail pour Android, vous pouvez recevoir des notifications par e-mail pour les sous-dossiers de votre compte de messagerie.

> **Remarque :**
>
> - Assurez-vous que la notification push FCM est activée dans la console Endpoint Management pour recevoir des notifications pour les sous-dossiers. Pour connaître la procédure de configuration des notifications push basées sur FCM, voir Notifications push pour Secure Mail.
> - La fonctionnalité de notification de sous-dossier n'est pas disponible pour Lotus Notes Server.

**Pour activer les notifications pour les sous-dossiers**

1. Accédez à **Paramètres** puis sous **Général**, appuyez sur **Notifications**.
2. Dans l'écran **Notifications**, appuyez sur **Dossiers de messagerie**. Une liste des sous-dossiers de la boîte de réception apparaît.

3. Appuyez pour sélectionner les sous-dossiers pour lesquels vous souhaitez recevoir des notifications. La boîte de réception est sélectionnée par défaut.

> **Remarque :**
>
> L'activation des notifications pour les sous-dossiers active la synchronisation automatique.

Pour désactiver les notifications de sous-dossiers, décochez les cases correspondant aux sous-dossiers pour lesquels vous ne souhaitez pas recevoir de notifications.

### Canaux de notification

Sur les appareils fonctionnant sous Android O ou version ultérieure, vous pouvez utiliser les paramètres de canal de notification pour gérer vos notifications par e-mail et calendrier. Cette fonctionnalité vous permet de personnaliser et de gérer vos notifications.

Pour configurer les notifications pour les rappels par e-mail ou calendrier, ouvrez Secure Mail et accédez à **Paramètres > Notifications** et sélectionnez l'option de notification souhaitée.

Vous pouvez ensuite naviguer vers **Gérer les notifications par e-mail** ou **Gérer les notifications de calendrier** pour gérer vos notifications par e-mail ou calendrier.

Vous pouvez également appuyer longuement sur l'icône de l'application Secure Mail sur votre appareil, sélectionner **Infos sur l'application** puis appuyer sur **Notifications**.

Si votre paramètre Vibreur était précédemment défini sur **En mode silencieux**, il revient au paramètre Vibreur par défaut (**Désactivé**), avec cette fonction.

> **Remarque :**
>
> La manière dont votre administrateur a configuré la stratégie MDX Contrôler les notifications de l'écran verrouillé détermine si les notifications sont disponibles sur l'écran verrouillé.

### Joindre des fichiers dans Android

Dans les versions 10.3.5 et ultérieures de Secure Mail, les utilisateurs ne peuvent pas joindre d'images directement à partir de la galerie d'applications lorsque la stratégie Échange de documents entrants (Ouvrir dans) est définie sur **Restreint**. Si vous souhaitez conserver cette stratégie définie sur **Restreint**, tout en autorisant les utilisateurs à ajouter des photos à partir de la galerie, suivez les étapes suivantes dans la console Endpoint Management.

1. Définissez **Bloquer la galerie** sur **Désactivé**.
2. Obtenez l'ID de package de la galerie pour les appareils. Exemples :

- **LG Nexus 5 :**
  com.google.android.gallery3d, com.google.android.apps.photos
- **Samsung Galaxy Note 3 :**
  com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.
- **Sony Expire :**
  com.sonyericsson.album, com.google.android.apps.photos
- **HTC :**
  com.google.android.apps.photos, com.htc.album
- **Huawei :**
  com.android.gallery3d, com.google.android.apps.photos

3. Rendez la stratégie masquée Liste blanche d'échange de documents entrants visible :
   - Téléchargez le fichier APK WorxMail et encapsulez le fichier avec le MDX Toolkit.
   - Recherchez le fichier .mdx sur votre ordinateur et modifiez le suffixe du fichier sur .zip.
   - Ouvrez le fichier .zip et localisez le fichier policy_metadata.xml.
   - Recherchez et modifiez l'élément InboundDocumentExchangeWhitelist de `PolicyHidden >**true**</PolicyHidden>` à `<PolicyHidden>**false**</PolicyHidden>`.
   - Enregistrez le fichier policy_metadata.xml.
   - Sélectionnez tous les fichiers dans ce dossier et compressez-les pour créer le fichier .zip.

     > **Remarque :**
     >
     > Ne compressez pas le dossier externe. Sélectionnez tous les fichiers à l'intérieur du dossier et compressez les fichiers sélectionnés.

   - Cliquez sur le fichier compressé.
   - Choisissez **Obtenir des infos** et rétablissez le suffixe du fichier sur .mdx.
4. Chargez le fichier .mdx modifié sur la console Endpoint Management et ajoutez la liste des ID de package de galerie à la stratégie Liste blanche d'échange de documents entrants qui est maintenant visible.

   Vérifiez que les ID de package sont séparés par des virgules :

   com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo
5. Enregistrez et déployez Secure Mail.

Les utilisateurs Android peuvent maintenant joindre une image à partir de la galerie d'applications.

#### Formats de fichiers pris en charge

Un X indique un format de fichier pouvant être connecté, affiché et ouvert dans Secure Mail.

| Format | iOS | Android |
|---|---|---|
| Vidéo : H.263 AMR NB codec_Mp4 | | X |
| Vidéo : H.263 AMR NB codec_3gp | | X |
| Vidéo : H.264 AAC codec_3gp | X | X |
| Vidéo : H.264 AAC codec_mp4 | X | X |
| Vidéo: H.264 Acclc codec_mp4 | X | X |
| GTM recorded_wmv | | X |
| AVI | | X |
| WAV | X | X |
| MP4 | X | X |
| 3GP | X | X |
| Flac | | X |
| AAC | X | X |
| M4A | X | X |
| 3GP (AMR-NB) | X | X |
| MP3 | X | X |
| WAV | X | X |
| OGG | | X |
| ICO | X | X |
| JPEG | X | X |
| PNG | X | X |
| TIF (page unique seulement) | X | |
| BMP | X | X |
| GIF | X | X |
| WebP | | X |
| .dot | X | X |
| PDF | X | |
| PPT | X | X |

| Format | iOS | Android |
|---|---|---|
| PPTX | X | X |
| DOC | X | X |
| DOCX | X | X |
| XLS | X | X |
| XLSM | X | X |
| XLSX | X | X |
| TXT | X | X |
| POT | X | X |
| HTM | X | X |
| HTML | X | X |
| ZIP | X | X |
| EML | X | X |

## Comptes Exchange multiples pour Android

Depuis **Paramètres** dans Secure Mail, vous pouvez maintenant ajouter plusieurs comptes de messagerie Exchange et basculer entre ces derniers. Cette fonctionnalité vous permet de surveiller vos mails, contacts et calendriers dans un même emplacement.

### Conditions préalables

Un nom d'utilisateur et un mot de passe sont requis pour configurer des comptes supplémentaires. Les configurations d'inscription ou de stockage automatique des informations d'identification s'appliquent uniquement au premier compte configuré dans l'application. Tapez le nom d'utilisateur et mot de passe pour tous les comptes supplémentaires.

- Si le premier compte que vous créez est basé sur certificats, vous ne pouvez pas ajouter d'autres comptes basés sur certificats.
- Pour autoriser d'autres comptes à se connecter à un domaine ou un serveur Exchange Server dans un réseau externe, vous devez définir le split tunneling sur **Activé** dans Citrix ADC.
- Secure Mail pour iOS prend uniquement en charge les serveurs de messagerie Exchange et Office 365.

**Pour ajouter un compte de messagerie Exchange pour Android**

1. Ouvrez Secure Mail, touchez l'icône d'hamburger et touchez l'icône **Paramètres**.
2. Sous **Comptes**, touchez **Ajouter un compte**.
3. Sur l'écran **Ajouter un compte**, entrez les informations d'identification du nouveau compte.

   Si vous le souhaitez, vous pouvez définir des valeurs pour les paramètres suivants :

   - **Période de sync. des messages :** touchez pour sélectionner une valeur pour la période de synchronisation des messages. La valeur définie indique le nombre de jours de courriers que Secure Mail synchronise. Votre administrateur définit la valeur par défaut.
   - **En faire mon compte par défaut :** touchez pour définir le nouveau compte en tant que compte par défaut. La valeur est **désactivée** par défaut.
4. Touchez **Connexion** pour créer le compte.

   Vous pouvez afficher le nouveau compte dans l'écran **Paramètres** sous le menu **Comptes**.

> **Remarque :**
>
> Les comptes supplémentaires doivent utiliser l'authentification basée sur Active Directory. Secure Mail ne prend pas en charge l'authentification basée sur certificats lors de la configuration de comptes multiples.

**Pour modifier un compte**

Vous pouvez modifier le mot de passe et la description d'un compte de messagerie pour Android.

1. Ouvrez Secure Mail, touchez l'icône d'hamburger et appuyez sur l'icône **Paramètres**.
2. Sous **Comptes**, touchez le compte que vous voulez modifier.
3. Dans l'écran **Compte**, modifiez les champs.
4. Touchez **Enregistrer** pour confirmer l'action ou touchez **Annuler** pour revenir sur l'écran **Paramètres**.

**Pour supprimer un compte pour Android**

1. Ouvrez Secure Mail, touchez l'icône d'hamburger et touchez l'icône **Paramètres**.
2. Sous **Comptes**, touchez le compte que vous voulez supprimer.
3. Dans l'écran **Détails du compte**, touchez **Supprimer le compte** en bas de l'écran ou touchez **Annuler** pour revenir sur l'écran **Paramètres**.
4. Touchez **Supprimer** pour confirmer l'action.

> **Remarque :**
>
> Si vous supprimez le compte par défaut, le compte suivant deviendra le compte par défaut.

**Pour définir un compte par défaut pour Android**

Secure Mail utilise le compte par défaut dans les scénarios suivants :

- **Composition d'e-mails :** le champ **De :** est automatiquement renseigné avec l'ID d'e-mail du compte par défaut.
- **Création d'événements de calendrier :** le champ **Organisateur** est automatiquement renseigné avec l'ID d'e-mail du compte par défaut.

Lorsque vous ajoutez un ou plusieurs comptes de messagerie, le premier compte que vous créez est le compte par défaut. Pour modifier le compte par défaut, accédez à **Paramètres** et touchez **Défaut** sous **Général**.

Dans l'écran **Compte par défaut**, touchez le compte que vous souhaitez définir comme compte par défaut.

**Paramètres de comptes Exchange multiples pour Android**

Si vous avez configuré plusieurs comptes Exchange, certains des paramètres Secure Mail sont disponibles pour chacun de ces comptes individuellement, alors que d'autres paramètres sont globaux. Les paramètres suivants sont spécifiques au compte :

- Mode par défaut
- Notifications
- Absent(e) du bureau
- Fréquence synchr. boîte de réception
- Période de sync.
- Synchr. messagerie
- S/MIME
- Fichiers hors connexion
- Signature
- Réponses rapides
- Synchroniser l'agenda
- Synchroniser les contacts
- Synchroniser avec les contacts locaux
- Exporter les paramètres

Ces paramètres apparaissent avec l'icône >. Touchez l'icône > pour afficher les comptes sur votre appareil.

Pour appliquer ce paramètre à un compte spécifique, développez un élément de paramètre en tapant sur **>**, puis sélectionnez le compte de messagerie.

### Écran de boîtes aux lettres

L'écran **Boîtes aux lettres** affiche tous les comptes que vous avez configures et offre les vues suivantes :

- **Tous les comptes :** contient des e-mails de tous les comptes Exchange que vous avez configurés.
- **Comptes individuels :** contient les e-mails et dossiers d'un compte individuel. Ces comptes s'affichent sous forme de liste que vous pouvez développer pour afficher les sous-dossiers.

Pour afficher vos boîtes aux lettres, ouvrez Secure Mail et touchez l'icône d'hamburger. Dans l'écran **Boîtes aux lettres**, touchez le compte pour développer les options.

La vue **Tous les comptes** affiche collectivement les e-mails de plusieurs de vos comptes, les actions suivantes utilisent l'adresse e-mail du compte principal ou par défaut :

- Nouveau message
- Nouvel événement

Pour modifier l'adresse e-mail de l'expéditeur lors de la composition d'un nouveau message à partir de la vue **Tous les comptes**, touchez l'adresse par défaut dans le champ **De :** et sélectionnez un compte différent des comptes de messagerie qui s'affichent.

> **Remarque :**
>
> La composition d'un e-mail à partir de la vue de conversation renseigne automatiquement le champ **De :** avec l'adresse e-mail à laquelle cette conversation est adressée.

### Comptes individuels

Le compte principal ou par défaut s'affiche toujours en premier suivi des autres comptes par ordre alphabétique.

Les comptes individuels affichent les sous-dossiers que vous avez créés.

Les actions suivantes sont limitées aux comptes individuels uniquement :

- Déplacement d'éléments.
- Rédaction d'e-mails à partir de la vue de conversation.
- Enregistrement des contacts.

## Contacts

Touchez l'icône **Contacts** dans la barre d'onglets, puis touchez l'icône d'hamburger en haut à droite de l'écran. L'écran **Contacts** affiche les éléments suivants :

- **Tous les contacts :** affiche tous les contacts de plusieurs comptes de messagerie. Cette option apparaît uniquement si plusieurs comptes de messagerie sont configurés.
- **Compte de messagerie individuel :** affiche les contacts se rapportant au compte de messagerie individuel que vous avez configuré.
- **Catégories :** affiche les catégories de contacts que vous avez peut-être créées ou sélectionnées dans la liste prédéfinie pour regrouper les contacts.

### Pour afficher le dossier de contacts

> **Remarque :**
>
> les sous-dossiers de contacts ne sont pas pris en charge sur Secure Mail pour Android. Si vous avez créé des dossiers ou des sous-dossiers pour vos contacts à l'aide de Microsoft Outlook, vous ne pouvez pas les afficher dans Secure Mail.

1. Dans l'écran des contacts :
    - Appuyez sur tous les contacts pour afficher tous les contacts de plusieurs comptes de messagerie.
    - Appuyez sur un compte de messagerie individuel pour afficher les contacts associés à un compte de messagerie particulier.
2. Appuyez sur les catégories pour afficher les contacts regroupés sous des catégories spécifiques. Vous pouvez choisir de regrouper les contacts en fonction d'une catégorie que vous créez ou de les regrouper dans une catégorie à partir d'une liste prédéfinie.

Vous pouvez synchroniser les contacts relatifs à un compte individuel avec vos contacts locaux.

### Pour synchroniser avec les contacts locaux

1. Ouvrez Secure Mail.
2. Touchez l'icône Paramètres, accédez à **Contacts > Synchroniser avec les contacts locaux**, puis touchez > pour développer le menu.
3. Dans l'écran **Synchroniser contacts locaux**, activez le compte dont vous voulez synchroniser les contacts.
4. Touchez **OK**.
5. Lorsque vous êtes invité à autoriser Secure Mail à accéder à vos contacts, touchez **OK**.

Vous avez exporté avec succès les contacts du compte.
Pour annuler cette opération, accédez à **Paramètres > Contacts > Synchroniser avec les contacts locaux** et touchez le commutateur en regard du compte pour désactiver cette fonctionnalité. Touchez **OK** pour confirmer l'action.

## Calendrier

Le calendrier affiche tous les événements se rapportant aux comptes sur votre appareil. Vous pouvez définir des couleurs pour les comptes individuels pour différencier les événements de calendrier relatifs aux comptes individuels.

> **Remarque :**
>
> La fonctionnalité de calendrier personnel est toujours associée à votre compte principal ou compte par défaut.

### Pour définir des couleurs pour les événements de calendrier

1. Touchez l'icône **Calendrier** dans la barre d'onglets de pied de page, puis touchez l'icône d'hamburger en haut à gauche.
   L'écran **Calendriers** affiche tous les comptes que vous avez configurés.
2. Touchez la couleur par défaut affichée à droite d'un compte Exchange.
   L'écran Couleurs affiche les couleurs disponibles pour ce compte.
3. Sélectionnez une couleur de votre choix et touchez **Enregistrer**.
4. Pour revenir à l'écran précédent, touchez **Annuler**.
   La couleur sélectionnée est définie pour tous les événements de calendrier relatifs à ce compte Exchange.

Lorsque vous créez une invitation ou un événement de calendrier, le champ **Organisateur** est automatiquement renseigné avec l'adresse e-mail du compte par défaut. Pour modifier le compte de messagerie, touchez cette adresse e-mail et sélectionnez un autre compte.

### Rechercher

Recherche Vous pouvez effectuer une recherche globale dans la vue **Boîtes aux lettres** ou la vue **Tous les contacts**. Cette action affiche les résultats appropriés après une recherche de tous les comptes dans l'application.

Toutes les recherches effectuées à partir d'un compte individuel affichent les résultats se rapportant à ce compte uniquement.

## Android Entreprise dans Secure Mail

Secure Mail et Secure Web pour Android sont compatibles avec Android Entreprise, anciennement appelé Android for Work.

### Conditions préalables

- Pour être en mesure d'utiliser cette fonctionnalité, assurez-vous que votre appareil exécute Android 5.0 ou version ultérieure.
- Pour les déploiements sur site, la propriété **afw.accounts** de Endpoint Management doit être définie sur **TRUE**.

Une fois que vous avez configuré Android Entreprise dans Endpoint Management, les applications de productivité mobiles sont disponibles sur votre appareil. L'icône Android Entreprise identifie les applications, comme illustré dans l'image suivante.

### Fonctionnalités compatibles avec Android Entreprise

Le tableau suivant répertorie les fonctionnalités de Secure Mail qui sont compatibles avec Android Entreprise.

| Fonctionnalité | Support |
|---|---|
| Détection automatique de Exchange Server | X |
| Secure Ticket Authority | X |
| Exporter contacts | X |
| Gestion des droits relatifs à l'information Microsoft | X |
| Notifications d'écran verrouillé | X |
| Synchronisation des messages | X |
| Classification de la messagerie | X |
| Signature et cryptage S/MIME | X |
| Service Firebase Cloud Messaging (FCM) | X |
| Authentification moderne (OAuth) | |
| Comptes Exchange multiples | X |
| Calendrier personnel | |
| Exporter les paramètres de messagerie | X |

| Fonctionnalité | Support |
|---|---|
| Appareils partagés | |
| Intégration de Endpoint Management avec Microsoft Intune/EMS | |
| Office 365 | X |
| LDAP Exchange Server 2010, 2013 et 2016 | X |
| Authentification par certificats (CBA) | |
| GoToMeeting | X |
| Skype Entreprise | |
| Liste de distribution personnelle | X |
| Compatibilité Citrix Files | X |
| Inscription à la messagerie à l'aide de l'authentification unique (Single Sign-On) | X |

Le tableau suivant répertorie les fonctionnalités de Secure Web compatibles avec Android Entreprise.

| Fonctionnalité | Support |
|---|---|
| Mode de navigation sécurisée | X |
| Mode VPN complet | X |
| Toutes les fonctionnalités des applications | X |
| Compatibilité avec Secure Mail | X |

## Limitations

- Si la stratégie de restrictions **Autoriser utilisation de la barre d'état** est définie **ON** pour Android Entreprise en mode Profil de travail, la progression d'exportation du calendrier et les notifications push ne s'affichent pas dans la barre d'état de Secure Mail pour Android. Toutefois, ces notifications sont visibles sur l'écran verrouillé lorsqu'elles sont autorisées. Pour plus d'informations, consultez la section Paramètres Android Entreprise.

# Intégration de Secure Mail avec Slack (Aperçu)

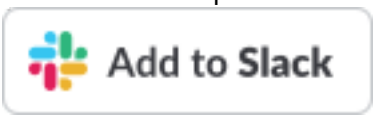
March 1, 2019

Vous pouvez désormais transférer vos conversations e-mail vers l'application Slack sur les appareils fonctionnant sous iOS ou Android.

Une fois que vous avez activé cette fonctionnalité, vous pouvez effectuer les opérations suivantes :

- Basculer facilement entre un e-mail et une conversation Slack
- Créer une conversation de groupe Slack avec vos destinataires de messagerie
- Créer un message direct dans Slack avec votre destinataire de messagerie

## Conditions préalables

- Pour les administrateurs :
  - vérifiez que vous avez installé Secure Mail dans votre espace de travail Slack. Cliquez sur le bouton **Ajouter à Slack** ci-dessous. 

  - Assurez-vous que la stratégie **Activer le jeu** est **Activée**. Pour plus de détails sur la stratégie, consultez les sections suivantes :
    * Activer la stratégie Slack pour iOS
    * Activer la stratégie Slack pour Android
- Pour les utilisateurs : avant de continuer, vérifiez que vous disposez d'un compte Slack et que l'application Slack est installée sur votre appareil.

## Pour activer cette fonctionnalité sur votre appareil

1. Ouvrez Secure Mail et touchez l'icône d'hamburger.
2. Dans l'écran **Boîtes aux lettres**, touchez l'icône des paramètres en bas à droite de l'écran.
3. Dans l'écran **Paramètres**, touchez l'option **Slack** répertoriée sous **Intégrations**.
4. Indiquez l'URL de votre espace de travail Slack, puis touchez **Continuer**.
5. Fournissez vos informations d'identification, puis touchez **Connexion**.
6. Lorsque vous êtes invité à autoriser l'accès Secure Mail à des informations, touchez **Autoriser**.

Vous êtes maintenant connecté à Slack.

### Pour utiliser cette fonctionnalité

1. Ouvrez une conversation e-mail dans Secure Mail, puis touchez le bouton d'action flottant.
2. Parmi les options disponibles, touchez **Chatter dans Slack**.
3. La conversation passe sur Slack avec les destinataires de votre messagerie.

**Gardez à l'esprit les considérations suivantes :**

- Sur les appareils exécutant Secure Mail pour iOS ou Android, vous pouvez créer une conversation Slack avec un maximum de huit destinataires à partir de votre messagerie. Si vous avez plus de huit destinataires dans votre messagerie, Secure Mail sélectionne par défaut les huit premiers destinataires présents dans votre conversation e-mail.

## Notifications et synchronisation

February 20, 2019

Cet article traite des fonctionnalités de synchronisation et de notification des courriers électroniques et des configurations pour Secure Mail.

### Actualisation en arrière-plan Secure Mail pour iOS

Si Secure Mail pour iOS est configuré pour fournir des notifications via l'actualisation de l'application en arrière-plan iOS (et non APNS), l'actualisation de la messagerie Secure Mail fonctionne comme suit :

- Lorsque l'utilisateur active l'**actualisation en arrière-plan** sur l'appareil à partir du menu **Paramètres** et que Secure Mail est exécuté en arrière-plan, les e-mails sont synchronisés avec le serveur. La fréquence de synchronisation dépend d'un certain nombre de facteurs.
- Si l'utilisateur désactive l'**actualisation en arrière-plan**, l'application ne reçoit jamais d'e-mail lorsqu'elle est exécutée en arrière-plan.
- Lorsque Secure Mail est exécuté en arrière-plan, l'application continue à fonctionner sans période de grâce avant qu'elle ne soit suspendue.
- Lors de l'exécution au premier plan, Secure Mail affiche l'activité de messagerie en temps réel, quelle que soit la manière dont le paramètre d'**actualisation en arrière-plan** est défini.

### Secure Mail et ActiveSync

Secure Mail se synchronise avec Exchange Server via le protocole de messagerie ActiveSync. Cette fonctionnalité fournit aux utilisateurs un accès en temps réel à leurs messages, contacts et événe-

ments de calendrier Outlook, boîtes aux lettres générées automatiquement et dossiers créés par eux-mêmes.

> **Remarque :**
>
> ActiveSync ne prend pas en charge la synchronisation des dossiers publics d'Exchange. Dans Exchange Server 2013, ActiveSync ne synchronise pas le dossier Brouillons.

Pour synchroniser des dossiers créés par les utilisateurs, suivez ces étapes :

#### iOS

1. Accédez à **Paramètres > Actualisation automatique**.
2. Définissez **Actualisation automatique** sur **Activé**.
3. Touchez **Activé**. Une liste de toutes les boîtes aux lettres s'affiche.
4. Touchez les dossiers que vous voulez synchroniser.

#### Android

1. Accédez à la liste des boîtes aux lettres.
2. Touchez la boîte aux lettres que vous voulez synchroniser.
3. Touchez l'icône Plus dans le coin inférieur droit.
4. Touchez **Options de synchronisation**.
5. Sous **Fréquence de consultation**, sélectionnez la fréquence à laquelle vous souhaitez synchroniser le dossier.

### Exportation des contacts dans Secure Mail

Les utilisateurs de Secure Mail peuvent synchroniser leurs contacts avec le répertoire téléphonique, effectuer une exportation ponctuelle d'un contact vers le répertoire ou partager un contact sous forme de pièce jointe vCard.

Pour activer ces fonctionnalités, définissez la stratégie Exporter contacts pour Secure Mail dans la console Endpoint Management sur **Activé**.

Lorsque la stratégie est **activée**, les options suivantes sont activées dans Secure Mail :

- **Synchroniser avec les contacts locaux** dans Paramètres
- Exportation de contacts individuels
- Partager des contacts en tant que pièces jointes vCard

Lorsque la stratégie Exporter contacts est **désactivée**, ces options n'apparaissent pas dans l'application.

Une fois que la stratégie est activée, pour synchroniser de manière continue les contacts depuis le serveur de messagerie vers le répertoire téléphonique, les utilisateurs doivent définir **Synchroniser avec les contacts locaux** sur **Activé**. Tant que **Synchroniser avec les contacts locaux** est définie sur **ACTIVÉ**, toute mise à jour des contacts dans Exchange ou Secure Mail entraîne une mise à jour des contacts locaux.

En raison de limites liées à Android, si un compte Exchange ou Hotmail est déjà défini pour se synchroniser avec des contacts locaux, Secure Mail n'est pas en mesure de synchroniser les contacts.

Sur iOS, les contacts Secure Mail peuvent être exportés et synchronisés avec les contacts du téléphone, même si Hotmail ou Exchange est configuré sur l'appareil des utilisateurs. Vous configurez cette fonctionnalité dans Endpoint Management via la stratégie Ignorer vérification des contacts pour Secure Mail. Cette stratégie détermine si Secure Mail ignore la vérification des contacts d'un autre compte Exchange/Hotmail configuré dans l'application Contacts native. Si elle est **activée**, l'application synchronise les contacts sur l'appareil même si l'application Contacts native est configurée avec un compte Exchange/Hotmail. Si elle est **désactivée**, l'application continue de bloquer la synchronisation des contacts. La valeur par défaut est **Activé**.

### Notifications Secure Mail

Le tableau suivant décrit la manière dont les notifications sont traitées pour les appareils mobiles pris en charge lorsque Secure Mail est exécuté au premier plan ou en arrière-plan.

| Avec Secure Mail exécuté au premier plan ou en arrière-plan : | Les notifications sont traitées pour iOS | Les notifications sont traitées pour Android |
|---|---|---|
| Au premier plan | Secure Mail maintient une connexion permanente à ActiveSync pour synchroniser les activités de messagerie et de calendrier. | Secure Mail maintient une connexion permanente à ActiveSync pour synchroniser les activités de messagerie et de calendrier. |
| En arrière-plan (ou terminé) | Secure Mail reçoit des notifications via la fonctionnalité d'actualisation de l'application en arrière-plan iOS ou, s'il est configuré, le service APNS. | Secure Mail maintient une connexion permanente à ActiveSync. |

Pour plus d'informations sur la configuration, veuillez consulter la section Notifications push pour Secure Mail pour iOS.

### Notifications push enrichies

Secure Mail pour iOS prend en charge les notifications Push enrichies. Grâce aux notifications enrichies, vous recevez des notifications d'écran de verrouillage pour votre boîte de réception même lorsque Secure Mail n'est pas exécuté en arrière-plan. Cette fonctionnalité est prise en charge avec les configurations d'authentification par mot de passe et d'authentification basée sur le client.

> **Remarque :**
>
> En raison de la modification de l'architecture effectuée pour prendre en charge cette fonctionnalité, les notifications par e-mail VIP uniquement ne sont plus disponibles.

Pour activer ces notifications push, assurez-vous que les conditions préalables suivantes sont remplies :

- Dans la console Endpoint Management, **activez** les notifications push.
- La stratégie Accès réseau est définie sur **Non restreint** ou **Tunnélisé vers le réseau interne**. Si votre stratégie Accès réseau est définie sur **Tunnélisé vers le réseau interne**, vérifiez que l'hôte EWS (Exchange Web Services) est configuré dans la stratégie Services réseau d'arrière-plan. Si les hôtes EWS et ActiveSync sont identiques, vérifiez que l'hôte ActiveSync est configuré dans la stratégie Services réseau d'arrière-plan.
- La stratégie Contrôler les notifications de l'écran verrouillé est définie sur **Autoriser** ou **Expéditeur de l'e-mail ou titre de l'événement**.
- Accédez à **Secure Mail > Paramètres > Notifications** et activez **Notifications par e-mail**.

Cette fonctionnalité n'est pas prise en charge si vous exécutez l'une des configurations suivantes :

- Authentification moderne à l'aide de Microsoft Office 365 (Oauth)
- Applications gérées par l'intégration de Endpoint Management avec Microsoft EMS/InTune
- Appareils inscrits à l'aide d'informations d'identification dérivées

### Raisons pour laquelle la notification « Vous avez un nouveau message » s'affiche sur les appareils iOS

La notification « Vous avez un nouveau message » s'affiche sur les appareils iOS lorsque Secure Mail ne reçoit pas de réponse des services web Exchange (EWS) dans le délai spécifié de 30 secondes requis pour récupérer les détails du message.

Vous pouvez également rencontrer ce problème sur votre appareil en raison d'une connectivité Wi-Fi ou de données médiocre.

Outre la réponse EWS différée, Secure Mail affiche également la notification « Vous avez un nouveau message » dans les situations suivantes :

- Lorsque Secure Mail ne parvient pas à lire les informations requises à partir du conteneur sécurisé. Ce scénario se produit généralement après le redémarrage de votre périphérique et avant son déverrouillage.
- Lorsque Secure Mail ne parvient pas à se connecter ou à configurer un canal sécurisé avec Citrix Gateway ou EWS.
- Lorsque vos informations d'identification ont expiré ou que vous avez modifié les informations d'identification, mais qu'elles ne sont pas encore mises à jour dans Secure Mail. La figure suivante montre la manière dont la notification apparaît dans ce scénario.
- Lorsque Secure Mail reçoit une réponse inattendue du serveur Exchange pour une demande valide provenant de Secure Mail. Pour plus d'informations sur les codes de réponse EWS, veuillez consulter la documentation Microsoft Developer.

### Messages d'échec de la notification push pour Secure Mail pour iOS

Dans Secure Mail pour iOS, les messages d'échec de notification push apparaissent dans le centre de notification de votre appareil. Ces notifications apparaissent en fonction du type d'échec de notification.

Les messages de notification suivants apparaissent en fonction de différents scénarios d'échec, comme suit :

- **Secure Mail ne peut pas se connecter au réseau de votre entreprise.** Cette notification apparaît lorsque Secure Mail ne parvient pas à établir une connexion SOCKS5 avec Citrix Gateway.
- **Secure Mail ne peut pas se connecter au réseau de votre entreprise. Contactez votre administrateur.** Cette notification s'affiche lorsque Citrix Gateway est inaccessible. Assurez-vous que votre Citrix ADC est correctement configuré et accessible depuis des réseaux externes.
- **Secure Mail ne parvient pas à se connecter de manière sécurisée au réseau de votre entreprise. Contactez votre administrateur**. Cette notification apparaît lorsque Secure Mail ne parvient pas à établir une connexion SSL avec Citrix Gateway. Assurez-vous que votre certificat SSL est valide.
- **Secure Mail ne peut pas se connecter de manière sécurisée à votre serveur de messagerie. Veuillez contacter votre administrateur**. Cette notification apparaît lorsque Secure Mail ne parvient pas à établir une connexion SSL avec Exchange Server. Assurez-vous que le certificat SSL sur votre serveur Exchange est valide. Si vous souhaitez que l'application se connecte au serveur Exchange malgré un certificat non valide, assurez-vous d'avoir activé la stratégie MDX Accepter tous les certificats SSL.
- **Secure Mail ne peut pas récupérer le message en raison d'une erreur du serveur de messagerie. Veuillez contacter votre administrateur**. Cette notification apparaît lorsque Secure Mail ne peut pas analyser la réponse EWS du serveur Exchange.

- **Secure Mail ne peut pas récupérer le message car la demande a expiré**. Cette notification apparaît lorsque Secure Mail ne reçoit pas de réponse du serveur dans les 30 secondes. Cette notification peut apparaître en raison d'une connexion Wi-Fi ou de données médiocre sur votre appareil. Réessayez après quelques minutes.
- **Impossible de récupérer le message. Veuillez ouvrir Secure Mail**. Cette notification apparaît lorsque Secure Mail ne peut pas lire vos informations d'identification à partir du conteneur sécurisé. Cette notification peut apparaître lorsque votre appareil a été redémarré mais pas encore déverrouillé. Déverrouillez votre appareil pour autoriser automatiquement Secure Mail à accéder au conteneur sécurisé. Si vous recevez toujours cette notification, ouvrez Secure Mail pour mettre à jour automatiquement vos informations d'identification dans le conteneur sécurisé.

## Notifications push pour Secure Mail

March 12, 2019

Secure Mail pour iOS et Secure Mail pour Android peuvent recevoir des notifications sur les activités de messagerie et de calendrier lorsque l'application est exécutée en arrière-plan ou qu'elle est fermée. Secure Mail pour iOS prend en charge les notifications fournies par le biais de la fonctionnalité Actualisation en arrière-plan ou des notifications push fournies via le Apple Push Notification Service (APNS). Secure Mail pour Android prend en charge les notifications fournies via le service Firebase Cloud Messaging (FCM).

### Fonctionnement des notifications push

Secure Mail envoie des notifications push pour les activités de boîte de réception suivantes :

- **Nouveau message, demandes de réunions, annulations de réunions, mises à jour de réunions :** lorsque APNS envoie des notifications à une boîte de réception, Secure Mail met à jour tous les dossiers, y compris le calendrier, de façon à ce que les modifications apportées aux réunions soient reflétées immédiatement dans les calendriers des utilisateurs.
- **Pour iOS, l'état de Secure Mail passe de lu à non lu et vice versa.** L'icône Secure Mail affiche le nombre total de messages non lus et de nouveaux messages dans le dossier Boîte de réception Exchange uniquement. Secure Mail actualise l'icône après lecture des messages sur un ordinateur de bureau où sur un ordinateur portable.

  Pour iOS, Secure Mail indique toujours le nombre de messages non lus dans la boîte de réception pour la période de synchronisation. Si la stratégie Contrôler les notifications de l'écran verrouillé est définie sur **Activé**, les notifications push apparaissent sur l'écran d'un appareil verrouillé après qu'iOS réveille Secure Mail pour effectuer une synchronisation.

Lors d'une installation ou d'une mise à niveau, Secure Mail pour iOS invite les utilisateurs à autoriser les notifications push. Les utilisateurs peuvent également autoriser les notifications push ultérieurement à l'aide des réglages iOS.

Pour fournir des notifications push pour iOS et Android, Citrix héberge un service d'écoute sur Amazon Web Services (AWS) pour exécuter les fonctions suivantes :

- Écouter les notifications push Exchange Web Services (EWS) envoyées par les serveurs Exchange en cas d'activité sur la boîte de réception. Exchange n'envoie pas le contenu des messages au service Citrix.

  Aucune information permettant de vous identifier personnellement n'est stockée par le service Citrix. Au lieu de cela, un jeton d'appareil et un ID d'abonnement identifient l'appareil et le dossier Boîte de réception à mettre à jour dans Secure Mail.

- Envoyer des notifications APNS, contenant uniquement le nombre de badges, à Secure Mail sur les appareils iOS.
- Envoyer des notifications FCM à Secure Mail sur les appareils Android.

Le service d'écoute Citrix n'affecte pas le trafic des données de messagerie, qui continuent de transiter entre les appareils des utilisateurs et les serveurs Exchange via ActiveSync. Le service d'écoute, qui est configuré pour une haute disponibilité et une récupération d'urgence, est disponible dans trois zones :

- Amériques
- Europe, Moyen-Orient et Afrique (EMEA)
- Asie-Pacifique (APAC)

### Configuration système requise pour les notifications push

Si votre configuration Citrix Gateway comprend une STA (Secure Ticket Authority) et que le split tunneling est désactivé, Citrix Gateway doit autoriser le trafic (lorsqu'il passe par un tunnel de Secure Mail) vers les URL suivantes du service d'écoute Citrix :

| Région | URL | Adresse IP |
|---|---|---|
| Amériques | `https://us-east-1.pushreg.xm.citrix.com` | 52.7.65.6 ; 52.7.147.0 |
| EMEA | `https://eu-west-1.pushreg.xm.citrix.com` | 54.154.200.233 ; 54.154.204.192 |
| APAC | `https://ap-southeast-1.pushreg.xm.citrix.com` | 52.74.236.173 ; 52.74.25.245 |

### Configuration de Secure Mail pour les notifications push

Pour configurer les notifications push Apple ou FCM pour Secure Mail pour la distribution sur des magasins d'applications, dans la console Endpoint Management, **activez** les notifications Push, puis sélectionnez votre région. La figure suivante montre le paramètre pour iOS.

Pour Android, la figure suivante montre le même **paramètre de notification push** que pour iOS. De plus, si les services web Exchange (EWS) sont hébergés dans une région différente de celle du serveur de messagerie, renseignez le paramètre **Nom d'hôte EWS**. Le paramètre par défaut est vide. Si vous laissez le paramètre vide, Endpoint Management utilise le nom d'hôte du serveur de messagerie.

Configurez Exchange et Citrix ADC afin de permettre la transmission du trafic au service d'écoute.

### Configuration du serveur Exchange

Autorisez le trafic SSL sortant (sur le port 443) depuis votre pare-feu vers l'URL du service d'écoute Citrix correspondant à la région où se trouve votre serveur Exchange. Par exemple :

| Région | URL | Adresse IP |
|---|---|---|
| Amériques | `https://us-east-1.mailboxlistener.xm.citrix.com` | 52.6.252.176 ; 52.4.180.132 |
| EMEA | `https://eu-west-1.mailboxlistener.xm.citrix.com` | 54.77.174.172 ; 52.17.147.220 |
| APAC | `https://ap-southeast-1.mailboxlistener.xm.citrix.com` | 52.74.231.240 ; 54.169.87.20 |

Si vous disposez d'un serveur proxy entre les services web Exchange (EWS) et le périphérique d'écoute de Citrix, vous pouvez effectuer l'une des opérations suivantes.

- Envoyer le trafic EWS via proxy, puis sur le périphérique d'écoute.
- Contourner le proxy et acheminer le trafic EWS directement vers le périphérique d'écoute.

Pour envoyer le trafic EWS via le serveur proxy, configurez le fichier web.config EWS dans le dossier ClientAccess\exchweb\ews comme suit.

```
1 <configuration>
2 <system.net>
3 <defaultProxy>
```

```
<proxy usesystemdefault="true" bypassonlocal="true" />
</defaultProxy>
</system.net>
</configuration>
```

Pour plus de détails sur la configuration des proxys, voir Configuration du proxy.

Pour les environnements Exchange 2013, vous devez ajouter la section `system.net` au fichier web.config manuellement. Sinon, les configurations décrites dans cet article devraient fonctionner pour Exchange 2013. Pour résoudre des problèmes, contactez votre administrateur Exchange.

Pour contourner le serveur proxy, configurez la liste de contournement pour autoriser Exchange à établir des connexions au service d'écoute Citrix.

Lorsque Secure Hub est inscrit avec l'authentification par certificat, vous devez également configurer Exchange Server pour l'authentification par certificat. Pour de plus amples informations, consultez l'article Concepts avancés de Endpoint Management.

### Configuration de Citrix Gateway

Alors que le serveur Exchange Server doit autoriser le trafic vers le service d'écoute, Citrix ADC doit autoriser le trafic vers le service d'enregistrement. Ceci permet aux appareils de se connecter afin de s'enregistrer pour les notifications push.

Si vos serveurs EWS et ActiveSync sont différents, configurez votre stratégie de trafic Citrix ADC afin d'autoriser le trafic EWS.

### Résolution des problèmes

Pour résoudre les problèmes de connexions sortantes, consultez les journaux d'événements Exchange, notamment les entrées de journal qui sont consignées lorsqu'une demande d'abonnement ou qu'une notification d'abonnement est non valide ou échoue. Vous pouvez également exécuter des traces Wireshark sur le serveur Exchange pour suivre le trafic sortant sur le service d'écoute Citrix.

Pour les autres problèmes, essayez l'outil Secure Mail Test Tool.

### Questions fréquemment posées sur les notifications push Secure Mail

#### Quand iOS envoie-t-il des notifications à Secure Mail

Si Secure Mail est en cours d'exécution au premier plan, les notifications sont *toujours* envoyées à Secure Mail. Il s'agit du seul scénario dans lequel Citrix peut garantir que les notifications sont envoyées.

Lorsque Secure Mail passe en arrière-plan, le nombre de badges d'application est toujours mis à jour. Toutefois, les notifications (notifications de verrouillage et de bannière) dépendent de l'actualisation en arrière-plan et - en particulier quand iOS interrompt ou ferme l'application - l'envoi de notifications n'est pas garanti. Les facteurs suivants échappent au contrôle de Citrix.

Les cas suivants peuvent affecter la remise de notifications :

- La batterie est faible.
- Secure Mail n'est pas utilisé fréquemment (rarement ouvert au premier plan).
- Les messages sont reçus en dehors des plages d'utilisation principales au cours desquelles l'application est suspendue pour une période prolongée en arrière-plan ; par exemple, entre minuit et 6 heures.

Les notifications *ne sont pas* envoyées à Secure Mail dans les cas suivants :

- Si l'utilisateur ferme Secure Mail, jusqu'à ce que l'utilisateur rouvre manuellement l'application.
- Si le système a fermé Secure Mail et l'application n'a pas été redémarrée automatiquement.
- Lorsque Secure Mail n'est pas actif.

> **Important :**
>
> Il est possible que les notifications ne soient pas remises à l'application Secure Mail lorsqu'elle n'est pas active pour de nombreuses raisons, y compris mais pas exclusivement dans les cas suivants :
>
> - Si l'appareil est en mode alimentation basse et que Secure Mail est en arrière-plan. Il s'agit du cas le plus fréquent dans lequel des notifications ne sont pas envoyées.
> - Si l'actualisation en arrière-plan est désactivée pour Secure Mail et si Secure Mail est en arrière-plan. Notez que les utilisateurs contrôlent ce paramètre.
> - Si la connectivité réseau de l'appareil est faible. Cette situation dépend entièrement de l'appareil iOS.

Lorsque Secure Mail ne reçoit pas de notification, Secure Mail ne synchronise pas les nouvelles données sur l'appareil. En conséquence, les situations suivantes se produisent :

- Secure Mail synchronise les données uniquement lorsque les utilisateurs placent l'application au premier plan.
- Les notifications de l'écran de verrouillage ne sont plus envoyées pour les nouveaux messages. Les rappels de calendrier s'affichent toujours.

#### Quand Android envoie-t-il des notifications à Secure Mail

Sur Android, les notifications sont toujours envoyées à Secure Mail.

### Comment FCM affecte-t-il les notifications de messages qui s'affichent sur l'écran de verrouillage

Les notifications de nouveaux messages qui apparaissent sur l'écran d'un appareil verrouillé sont générées sur la base des données qui sont synchronisées sur l'appareil par Secure Mail. En outre, ces informations ne proviennent pas du service d'écoute.

Pour afficher les notifications de nouveaux messages, Secure Mail doit être en mesure de synchroniser les données à partir d'Exchange afin que Secure Mail dispose des informations pour créer les notifications.

Lorsque vous recevez un nouveau message, la notification FCM **Vous avez de nouveaux messages** s'affiche. Une fois la synchronisation des messages terminée en arrière-plan, le nouveau message apparaît dans Secure Mail.

### Comment l'actualisation en arrière-plan affecte-t-elle Secure Mail et APNS

Si l'utilisateur désactive l'actualisation en arrière-plan, les situations suivantes se produisent :

- Secure Mail ne reçoit pas de notifications lorsque Secure Mail n'est pas l'application en arrière-plan.
- Secure Mail n'actualise pas l'écran de verrouillage avec les notifications de nouveaux messages.

La désactivation de l'actualisation en arrière-plan a d'importantes répercussions sur le comportement de Secure Mail. Comme indiqué précédemment, les mises à jour de badges (pastilles) basées sur APNs ont toujours lieu, mais aucun message n'est synchronisé sur l'appareil dans ce mode.

### Comment le mode alimentation basse affecte-t-il Secure Mail et APNS

Le comportement du système vis-à-vis de Secure Mail est le même en Mode alimentation basse que lorsque l'Actualisation en arrière-plan est désactivée. En Mode alimentation basse, l'appareil ne « réveille » pas les applications pour les actualisations périodiques et n'envoie pas de notifications aux applications en arrière-plan. Les effets secondaires sont donc les mêmes que ceux répertoriés dans la section Actualisation en arrière-plan ci-dessus. Veuillez noter qu'en mode alimentation basse, les mises à jour de badges (pastilles) ont toujours lieu, basées sur les notifications APNs.

### Comment APNS affecte-t-il les notifications de messages qui s'affichent sur l'écran de verrouillage

Les notifications de nouveaux messages qui apparaissent sur l'écran d'un appareil verrouillé sont générées sur la base des données qui sont synchronisées sur l'appareil par Secure Mail. En outre, ces informations ne proviennent pas du service d'écoute.

Pour afficher les notifications de nouveaux messages, Secure Mail doit être en mesure de synchroniser les données à partir d'Exchange afin que Secure Mail dispose des informations pour créer les notifications.

Si les notifications APNs ne sont pas envoyées à Secure Mail en arrière-plan, Secure Mail ne détecte pas les notifications et, par conséquent, ne synchronise pas les nouvelles données. Étant donné qu'aucune nouvelle donnée n'est envoyée à Secure Mail, aucune notification de message n'est générée sur l'écran de verrouillage de l'appareil, même lorsque des notifications APNS ne sont pas transmises.

#### Quels autres problèmes peuvent provoquer l'échec de la synchronisation FCM en arrière-plan

Un certain nombre de problèmes peuvent provoquer l'échec des demandes de synchronisation FCM, y compris ce qui suit :

- Un ticket STA non valide.
- Lorsque Secure Mail est réveillé du mode de veille, l'application dispose de 10 secondes pour synchroniser toutes les données à partir du serveur.

Si l'une des conditions précédentes se produit, Secure Mail ne peut pas synchroniser les données. Par conséquent, les notifications ne s'affichent pas sur l'écran de verrouillage.

#### Quels autres problèmes peuvent provoquer l'échec de la synchronisation APNS en arrière-plan

Un certain nombre de problèmes peuvent provoquer l'échec des demandes de synchronisation APNS, y compris ce qui suit :

- Un ticket STA non valide.
- Une connexion réseau lente. Lorsque Secure Mail est activé en arrière-plan, l'application dispose de 30 secondes pour synchroniser toutes les données à partir du serveur.
- Si la stratégie de protection des données est activée et que Secure Mail est activé par une notification APNs, lorsque l'appareil est verrouillé, Secure Mail ne peut pas accéder au magasin de données et la synchronisation ne se produit pas. Notez qu'il s'agit du seul cas dans lequel le système tente de démarrer à froid Secure Mail. Si un utilisateur a déjà démarré Secure Mail à un moment donné après avoir déverrouillé l'appareil, la synchronisation APNs réussit même lorsque l'appareil est verrouillé.

Si l'une de ces conditions se produit, Secure Mail ne peut pas synchroniser les données et, par conséquent, il ne peut pas afficher les notifications sur l'écran de verrouillage.

### De quelle autre façon Secure Mail génère-t-il des notifications de l'écran de verrouillage lorsque les notifications ne sont pas transmises ou qu'APNS n'est pas exécuté

Si le service APNs est désactivé, Secure Mail est toujours activé par des événements d'actualisation en arrière-plan périodiques d'iOS, en supposant que l'actualisation en arrière-plan est activée et que le Mode alimentation basse est désactivé.

Au cours de ces événements de mise en éveil, Secure Mail synchronise les nouveaux messages depuis Exchange Server. Ces nouveaux messages peuvent être utilisés pour générer des notifications sur l'écran de verrouillage. Par conséquent, même lorsque les notifications APNs ne sont pas délivrées ou que APNs est désactivé, Secure Mail peut synchroniser les données en arrière-plan.

Il est important de noter que les synchronisations sont moins fréquentes en temps réel que lorsqu'APNs est en cours d'utilisation et que des notifications APNs sont transmises à Secure Mail. Quand iOS achemine des notifications APNs à Secure Mail, l'application synchronise immédiatement les données depuis le serveur et les notifications de l'écran de verrouillage s'affichent en temps réel.

Dans l'éventualité où des mises en éveil de l'actualisation en arrière-plan sont requises, les notifications de l'écran de verrouillage ne s'affichent pas en temps réel. Dans ce cas, Secure Mail est activé à une fréquence déterminée exclusivement par iOS. C'est la raison pour laquelle un délai peut s'écouler entre la remise d'un message dans la boîte de réception d'un utilisateur sur Exchange et le moment où Secure Mail synchronise ce message et génère la notification sur l'écran de verrouillage.

Notez également que Secure Mail reçoit ces mises en éveil périodiques même lorsque APNs est en cours d'utilisation. Dans tous les cas dans lesquels l'actualisation en arrière-plan met en éveil Secure Mail, Secure Mail tente de synchroniser les données depuis Exchange.

### En quoi Secure Mail diffère-t-il des autres applications qui affichent du contenu sur l'écran de verrouillage

Une différence très importante - et qui peut prêter à confusion - est que Secure Mail n'affiche pas toujours les nouveaux messages en temps réel sur l'écran de verrouillage de la même façon que Gmail, Microsoft Outlook et d'autres applications. La raison principale pour cette différence est la sécurité. Pour s'aligner avec le comportement des autres applications, le service d'écoute Citrix exigerait les informations d'identification de l'utilisateur pour s'authentifier auprès d'Exchange afin d'obtenir le contenu du message et transmettre ce contenu via le service d'écoute Citrix, ainsi que le service APNs d'Apple. L'approche de Citrix en matière de notifications APNs n'exige pas que le service d'écoute Citrix acquiert ou stocke le mot de passe des utilisateurs. Le service d'écoute n'a pas accès à la boîte aux lettres ni au mot de passe des utilisateurs.

Remarque sur l'application de messagerie iOS native : iOS permet à sa propre application de messagerie de maintenir une connexion permanente avec le serveur de messagerie, ce qui garantit que

les notifications sont toujours envoyées. Les applications tierces en dehors de la messagerie native ne sont pas autorisées à utiliser cette fonctionnalité.

**Comportement de l'application Gmail :** Google possède et contrôle l'application Gmail et le serveur Gmail. Cela signifie que Google peut lire le contenu du message et inclure ce contenu dans la charge utile de notification d'APNs. Lorsque iOS reçoit cette notification APNs de Gmail, iOS effectue les opérations suivantes :

- Définit le badge d'application en fonction de la valeur spécifiée dans la charge utile de notification.
- Affiche la notification sur l'écran de verrouillage à l'aide du texte du message qui est contenu dans la charge utile de notification.

Importante distinction : c'est iOS, et non l'application Gmail, qui affiche la notification de l'écran de verrouillage, en fonction des données contenues dans la charge utile. En fait, iOS peut ne jamais mettre en éveil l'application Gmail, de la même façon qu'iOS peut ne jamais mettre en éveil Secure Mail lors de la réception d'une notification. Toutefois, étant donné que la charge utile contient un extrait du message, iOS peut afficher la notification de l'écran de verrouillage sans qu'aucune donnée de message ne soit synchronisée sur l'appareil.

Dans Secure Mail, cette situation est différente. Secure Mail doit d'abord synchroniser les données du message à partir d'Exchange avant que l'application ne puisse pas afficher la notification de l'écran de verrouillage.

**Comportement de l'application Outlook pour iOS :** Microsoft contrôle Outlook pour iOS. Toutefois, l'organisation à laquelle l'utilisateur appartient, contrôle les serveurs Exchange à partir desquels les données sont obtenues. En dépit de cette configuration, Outlook peut afficher les notifications de l'écran de verrouillage en fonction des données que Microsoft fournit dans la notification APNs, car Outlook pour iOS utilise un modèle dans lequel Microsoft stocke les informations d'identification de l'utilisateur. Microsoft accède directement à la boîte aux lettres de l'utilisateur à partir de son service cloud et détermine la présence de nouveaux messages.

Si un nouveau message est disponible, le service cloud de Microsoft génère une notification APNs qui contient les nouvelles données de message. Ce modèle fonctionne de façon analogue au modèle Gmail dans lequel iOS récupère simplement les données et génère une notification d'écran de verrouillage en fonction de ces données. L'application iOS Outlook n'est pas impliquée dans le processus.

**Remarque de sécurité importante sur Outlook pour iOS :** l'approche Outlook pour iOS a des répercussions sur la sécurité. Les organisations doivent faire confiance à Microsoft car les mots de passe de leurs utilisateurs sont transmis à Microsoft afin qu'il puisse accéder aux boîtes aux lettres des utilisateurs, ce qui constitue un risque pour la sécurité. Pour plus d'informations sur la façon dont Microsoft gère les mots de passe des utilisateurs, consultez Microsoft TechNet.

Pour accéder aux questions fréquentes sur les notifications push spécifiques aux administrateurs, consultez cet article du Centre de connaissances. Pour accéder à des questions fréquentes spécifiques

aux utilisateurs, consultez cet article du centre de connaissances.

## Interactivité de Secure Mail avec d'autres applications de productivité mobiles et Citrix Files

February 19, 2019

L'interactivité de Secure Mail avec d'autres applications de productivité mobiles et Citrix Files permet aux utilisateurs d'accéder, modifier, partager et enregistrer des documents de manière transparente, sans quitter l'environnement sécurisé défini par les stratégies de votre organisation. Par exemple, le fait de toucher un lien dans Secure Mail ouvre le site dans Secure Web. Les utilisateurs peuvent ouvrir et modifier des pièces jointes avec Citrix QuickEdit pour Endpoint Management. Les pièces jointes sont téléchargées sur l'espace Citrix Files pour Endpoint Management de l'utilisateur.

Pour obtenir une liste complète des fonctionnalités de Secure Mail pour chaque plate-forme, consultez la section Fonctionnalités par plate-forme.

## Test et dépannage de Secure Mail

March 1, 2019

Lorsque Secure Mail ne fonctionne pas correctement, cela est généralement causé par des problèmes de connexion. Cet article explique comment éviter les problèmes de connexion. Si des problèmes se produisent, cet article explique comment les résoudre.

### Test des connexions ActiveSync, authentification utilisateur et configuration APNS

Vous pouvez utiliser Endpoint Management Analyzer pour procéder à des vérifications du service de détection automatique de Secure Mail. Il vous explique comment télécharger l'application Endpoint Management Exchange ActiveSync Test. L'option de test de la messagerie (Mail test) dans XenMobile Analyzer vérifie les paramètres de connexion de base du serveur de messagerie. Cet outil veille également à ce que les serveurs ActiveSync soient prêts en vue de leur déploiement dans un environnement Endpoint Management. Pour plus d'informations, consultez Endpoint Management Analyzer Tool.

L'option Mail test dans Analyzer vérifie ce qui suit :

- Les connexions iOS et Android avec les serveurs Microsoft Exchange ou IBM Traveler.
- L'authentification utilisateur.

- La configuration de notification push pour iOS, y compris Exchange Server, Exchange Web Services (EWS), Citrix Gateway, les certificats APNs et Secure Mail. Pour de plus amples informations sur les notifications push, consultez la section Notifications push pour Secure Mail pour iOS.

L'outil fournit une liste complète des recommandations visant à résoudre les problèmes.

> Remarque :
>
> L'application Mail Test, MailTest.ipa, est obsolète. Accédez à la même fonctionnalité dans Endpoint Management Analyzer.

#### Exigences requises pour le test

- Assurez-vous que la stratégie d'accès réseau n'est pas bloquée.
- Définissez la stratégie Bloquer la composition d'e-mail sur **Désactivé**.

### Utilisation des journaux de Secure Mail pour résoudre les problèmes de connexion

Pour obtenir les journaux Secure Mail, procédez comme suit.

1. Accédez à **Secure Hub > Aide > Signaler un problème**.
2. Sélectionnez **Secure Mail** à partir de la liste des applications.

   Un e-mail adressé au service d'assistance de votre organisation s'affiche.
3. Remplissez la ligne d'objet et le corps avec quelques termes décrivant votre problème.
4. Sélectionnez le moment auquel le problème s'est produit.
5. Modifiez les paramètres de journal uniquement si votre équipe de support technique vous a demandé de le faire.
6. Cliquez sur **Envoyer**.

   Le message s'ouvre avec les fichiers journaux zippés en pièce jointe.
7. Cliquez de nouveau sur **Envoyer**.

   Les fichiers zip envoyés comprennent les journaux suivants :

   CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt et WH_logx.txt (Windows Phone)

Les journaux d'informations sur l'application contiennent des informations sur l'appareil et l'application. Vérifiez que le modèle du matériel et la version de la plate-forme sont pris en charge. Vérifiez que les versions de Secure Mail et du MDX Toolkit sont les plus récentes et qu'elles sont

compatibles. Pour de plus amples informations, consultez la section Configuration requise pour Secure Mail et Compatibilité Endpoint Management.

- CtxLog_VPNConfig.xml (iOS) et VpnConfig.xml (Android)

Les journaux de configuration VPN sont uniquement fournis pour Secure Hub. Vérifiez la version de Citrix ADC `ServerBuildVersion` pour vous assurer que la dernière version de Citrix ADC est utilisée. Vérifiez les paramètres `SplitDNS` et `SplitTunnel` comme suit :

- Si le split DNS est défini sur **Remote**, **Local** ou **Both**, vérifiez que vous avez correctement résolu le nom de domaine complet (FQDN) du serveur de messagerie via le DNS. (Le split DNS est disponible pour Secure Hub sur Android).
- Si le split tunnel est défini sur **Activé**, assurez-vous que votre serveur de messagerie est répertorié comme l'une des applications Internet accessibles sur le serveur principal.
- CtxLog_AppPolicies.xml (iOS), Policy.xml (Android et Windows Phone)

Les journaux des stratégies fournissent les valeurs de toutes les stratégies MDX appliquées à Secure Mail au moment où vous avez obtenu le journal. Pour les problèmes de connexion, vérifiez les valeurs des stratégies <`BackgroundServices`> et <`BackgroundServicesGateway`>.

- Journaux de diagnostic (dans le dossier de diagnostics)

Pour les configurations initiales de Secure Mail, le problème le plus courant est « Votre réseau d'entreprise n'est pas disponible pour le moment. » Pour utiliser les journaux de diagnostic pour résoudre les problèmes de connexion, procédez comme suit.

Les colonnes clés des journaux de diagnostic sont Timestamp, Message Class et Message. Lorsqu'un message d'erreur s'affiche dans Secure Mail, prenez note de l'heure de façon à pouvoir localiser rapidement les entrées de journal correspondantes dans la colonne **Timestamp**.

Pour déterminer si l'appareil s'est bien connecté à Citrix Gateway, passez en revue les entrées AG Tunneler. Les messages suivants indiquent que la connexion a réussi :

- AG policy Intercepting FQDN:443 for STA tunneling
- New TCP proxy connection to (null):443 established

Pour déterminer si Citrix Gateway a bien réussi à se connecter à Endpoint Management (et peut donc valider le ticket STA), procédez comme suit : consultez le journal des diagnostics de Secure Hub et vérifiez les entrées INFOS (4) sous Message Class, à l'heure à laquelle l'appareil a été inscrit. Les messages suivants indiquent que Secure Hub a obtenu un ticket STA de Endpoint Management :

- Getting STA Ticket.
- Got STA Ticket response.
- STA Ticket – Success obtaining STA ticket for App – Secure Mail.

> Remarque :
>
> Au cours de l'inscription, Secure Hub envoie une requête de ticket STA à Endpoint Management. Endpoint Management envoie le ticket STA à l'appareil, où il est stocké et ajouté à la liste des tickets STA Endpoint Management.

Pour déterminer si Endpoint Management a émis un ticket STA pour un utilisateur, sélectionnez User-AuditLogFile.log, inclus dans le pack de support. Il répertorie la date et l'heure à laquelle le problème s'est produit, le nom d'utilisateur, les machines utilisateur et le résultat pour chaque ticket. Par exemple :

**Heure :** 2015-06-30T 12:26:34.771-0700

**Utilisateur :** user2

**Appareil :** Mozilla/5.0 (iPad; CPU OS 8_1_2 like macOS)

**Résultat :** ticket STA généré avec succès pour l'utilisateur « utilisateur2 » pour l'application « Secure Mail »

Pour vérifier les communications entre Citrix Gateway et le serveur de messagerie, vérifiez si le DNS et le réseau sont correctement configurés. Pour ce faire, utilisez Secure Web pour accéder à Outlook Web Access (OWA). À l'instar de Secure Mail, Secure Web peut utiliser un tunnel micro VPN pour établir une connexion à Citrix Gateway. Secure Web agit en tant que proxy vers la ressource interne ou externe à laquelle accède l'application. Dans la plupart des cas, notamment dans un environnement Exchange, OWA est hébergé sur le serveur de messagerie.

Pour tester la configuration, ouvrez Secure Web et entrez le nom de domaine complet de la page OWA. Cette requête utilise la même route et la même résolution DNS que les communications entre Citrix Gateway et le serveur de messagerie. Si la page OWA s'ouvre, vous savez que Citrix Gateway communique avec le serveur de messagerie.

Si les tests précédents indiquent que les communications sont bien établies, vous savez que le problème ne provient pas de votre installation Citrix. Le problème est plutôt lié aux serveurs Exchange ou Traveler.

Vous pouvez collecter des informations pour les administrateurs de vos serveurs Exchange ou Traveler. Commencez par rechercher la présence de problèmes HTTP sur les serveurs Exchange ou serveurs en recherchant le mot « Error » dans le journal de diagnostic de Secure Mail. Si des erreurs comprennent des codes HTTP et que vous disposez de plusieurs serveurs Exchange ou Traveler, examinez chaque serveur. Exchange et Traveler disposent de journaux HTTP qui affichent les requêtes et les réponses HTTP des machines clientes. Le journal d'Exchange se trouve dans C:\inetpub\LogFiles\W3SVC1\U_EX.log. Le journal de Traveler est IBM_TECHNICAL_SUPPORT>HTTHR.log.

### Pour obtenir des journaux d'incidents à partir d'un appareil pour Secure Mail pour iOS

1. Sur votre appareil iOS, accédez à **Réglages** > **Confidentialité** > **Analyse** > **Données d'analyse**.
2. Dans la liste **Données**, cliquez sur le nom de l'application et l'horodatage correspondant. Les journaux apparaissent.

### Résolution des problèmes liés à la messagerie, aux contacts ou au calendrier

Vous pouvez dépanner les problèmes de Secure Mail, tels que des e-mails bloqués dans les brouillons, des contacts manquants ou des éléments de calendrier non synchronisés. Pour résoudre ces problèmes, utilisez les journaux de la boîte aux lettres Exchange ActiveSync. Les journaux affichent les requêtes entrantes envoyées par les appareils et les réponses du serveur de messagerie.

Pour plus de détails, consultez la publication du blog TechNet Under the Hood: Exchange ActiveSync Mailbox Log Analysis.

### Recommandations pour la synchronisation illimitée

Lorsque les utilisateurs configurent leur période de synchronisation des messages sur **Tout**, la synchronisation est illimitée. Avec une synchronisation illimitée, il est supposé que les utilisateurs gèrent la taille de leur boîte aux lettres, qui comprend la boîte de réception et tous les sous-dossiers synchronisés. Voici quelques points à prendre en compte pour de meilleures performances.

1. Si la taille de la boîte aux lettres est supérieure à 18 000 messages ou 600 Mo, la synchronisation peut ralentir.
2. Il n'est pas recommandé d'activer **Charger les pièces-jointes par Wi-Fi** avec une synchronisation illimitée. Avec cette option, la taille des messages peut très rapidement engorger l'appareil.
3. Pour empêcher les utilisateurs de pouvoir sélectionner l'option de synchronisation illimitée, définissez la stratégie **Intervalle de synchronisation maximal** de l'application sur une valeur autre que **Tous**.
4. Il n'est pas recommandé de définir **Intervalle de synchronisation par défaut** sur **Tous** pour les utilisateurs.

**Locations**
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States