# BlackBerry UEM

## E-mail, calendrier et contacts

Administration

12.16

# Table des matières

# Configuration d'une messagerie professionnelle pour les terminaux

Vous pouvez utiliser l'une des options suivantes pour permettre aux utilisateurs de lire et d'envoyer des e-mails professionnels sur les terminaux :

- Vous pouvez utiliser BlackBerry Work pour gérer les e-mails, le calendrier et les contacts pour les terminaux des utilisateurs. Pour plus d'informations sur la gestion de BlackBerry Work, consultez la section Gestion des applications BlackBerry Dynamics et le Guide d'administration de BlackBerry Work.
- Vous pouvez utiliser les profils de messagerie pour spécifier la manière dont les terminaux se connectent au serveur de messagerie de votre organisation et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide de Exchange ActiveSync ou IBM Notes Traveler
- Vous pouvez également utiliser les profils de messagerie IMAP/POP3 pour spécifier la manière dont les terminaux se connectent aux serveurs de messagerie IMAP ou POP3 et synchronisent les e-mails.

# Désignation des terminaux autorisés à accéder à Exchange ActiveSync

Si votre organisation utilise Microsoft Exchange ActiveSync, vous pouvez empêcher les terminaux non autorisés d'utiliser Exchange ActiveSync sauf s'ils sont ajoutés expressément à la liste des terminaux autorisés. Les terminaux qui ne sont pas sur la liste autorisée ne peuvent pas accéder aux e-mails professionnels ni aux données de l'organiseur. BlackBerry Gatekeeping Service vous permet d'ajouter des terminaux à la liste autorisée en toute simplicité. Vous pouvez utiliser le système BlackBerry Gatekeeping Service, que vous utilisiez des profils de messagerie ou des applications BlackBerry Dynamics pour gérer l'accès aux e-mails, au calendrier et aux contacts sur les terminaux des utilisateurs.

Pour utiliser BlackBerry Gatekeeping Service, vous devez créer une configuration de contrôle pour Microsoft Exchange Server ou Microsoft Office 365, attribuer un profil de contrôle et configurer un profil de messagerie ou BlackBerry Work qui référence le serveur de contrôle d'accès automatique.

Une fois que vous avez configuré BlackBerry UEM pour pouvoir utiliser BlackBerry Gatekeeping Service, les terminaux des utilisateurs sont automatiquement ajoutés à la liste autorisée. Si le profil de contrôle d'accès, le profil de messagerie ou l'application de messagerie d'un utilisateur est supprimé, le terminal correspondant est supprimé de la liste autorisée et ne peut plus se connecter à Microsoft Exchange, sauf si vous l'autorisez par un autre moyen (par exemple, Windows PowerShell).

La plupart des terminaux ne permettent d'ajouter qu'un seul client de messagerie à la liste autorisée pour chaque terminal. Pour les terminaux Android Enterprise et Samsung Knox qui utilisent une configuration d'application contenant des données de liste blanche Exchange Server, la priorité de la liste blanche d'applications de messagerie est la suivante :

1. Applications de messagerie avec des configurations d'applications qui contiennent des données de liste blanche Exchange Server
2. BlackBerry Work
3. Client de messagerie pour lequel l'ID Exchange ActiveSync est envoyé lors de l'inscription

Si votre organisation utilise BlackBerry UEM dans un environnement sur site, vous pouvez installer une ou plusieurs instances de BlackBerry Connectivity Node pour ajouter des instances supplémentaires de composants de connectivité de terminal au domaine de votre organisation. Chaque BlackBerry Connectivity Node contient une instance de BlackBerry Gatekeeping Service. Chaque instance doit être en mesure d'accéder au serveur de contrôle d'accès de votre organisation. Si vous souhaitez que les données de contrôle d'accès soient gérées uniquement par l'instance de BlackBerry Gatekeeping Service installée avec les composants principaux de BlackBerry UEM, vous pouvez modifier les paramètres par défaut pour désactiver l'instance de BlackBerry Gatekeeping Service dans chaque instance de BlackBerry Connectivity Node. Pour plus d'informations sur l'installation et la configuration de BlackBerry Connectivity Node, reportez-vous au contenu relatif à la planification et au contenu relatif à l'installation et à la mise à niveau.

Si votre organisation utilise BlackBerry UEM Cloud, vous pouvez installer une ou deux instances de BlackBerry Connectivity Node pour ajouter des instances supplémentaires de composants de connectivité de terminal au domaine de votre organisation. Chaque BlackBerry Connectivity Node contient une instance de BlackBerry Gatekeeping Service. Chaque instance doit être en mesure d'accéder au serveur Exchange ActiveSync de votre entreprise. Si vous souhaitez gérer les paramètres d'accès de Exchange ActiveSync exclusivement par le BlackBerry Gatekeeping Service qui est installé avec le BlackBerry Connectivity Node principal, vous pouvez modifier les paramètres par défaut de façon à désactiver le BlackBerry Gatekeeping Service dans les autres instances de BlackBerry Connectivity Node. Pour plus d'informations sur l'installation et la configuration de BlackBerry Connectivity Node, reportez-vous à la section Installation ou mise à niveau de BlackBerry Connectivity Node dans le contenu relatif à la configuration de BlackBerry UEM Cloud.

Vous pouvez configurer des groupes de serveurs pour qu'ils dirigent le trafic de connectivité des terminaux vers une connexion locale spécifique à BlackBerry Infrastructure. Lorsque vous associez un profil de contrôle d'accès

à un groupe de serveurs, tout utilisateur auquel est attribué ce profil de contrôle d'accès utilise n'importe quelle instance active de BlackBerry Gatekeeping Service dans ce groupe de serveurs. Lorsque vous configurez un groupe de serveurs, vous pouvez choisir de désactiver les instances de BlackBerry Gatekeeping Service dans le groupe.

# Étapes de configuration d'Exchange ActiveSync et de BlackBerry Gatekeeping Service

Pour configurer BlackBerry Gatekeeping Service, procédez comme suit :

| Étape | Action |
|---|---|
| 1 | Configurer des autorisations à des fins de contrôle d'accès. |
| 2 | Autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync. |
| 3 | Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès. |
| 4 | Créer une configuration de contrôle d'accès. |
| 5 | Créez un profil de contrôle d'accès et attribuez-le aux comptes d'utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux. |

# Configurer des autorisations à des fins de contrôle d'accès

Pour utiliser le contrôle d'accès Exchange ActiveSync, vous devez créer un compte d'utilisateur dans Microsoft Exchange Server ou Microsoft Office 365 et lui donner les autorisations nécessaires pour le contrôle d'accès.

Si vous utilisez Microsoft Office 365, créez un compte d'utilisateur Microsoft Office 365 et attribuez-lui les rôles Destinataires de messagerie et Accès client dans l'entreprise.

Si vous utilisez Microsoft Exchange Server, suivez les instructions ci-dessous pour configurer les rôles de gestion avec les autorisations appropriées afin de gérer les boites aux lettres et l'accès client pour Exchange ActiveSync. Pour exécuter cette tâche, vous devez être un administrateur Microsoft Exchange doté des autorisations suffisantes pour créer et modifier les rôles de gestion.

**Avant de commencer :**

- Sur l'ordinateur qui héberge Microsoft Exchange, créez un compte et une boite aux lettres pour gérer le contrôle d'accès dans BlackBerry UEM (par exemple, BUEMAdmin). Vous devez spécifier les informations de connexion de ce compte lors de la création d'une configuration Exchange ActiveSync. Notez le nom de ce compte, vous devrez l'indiquer à la fin de la tâche ci-dessous.
- WinRM doit être configuré sur les paramètres par défaut sur l'ordinateur qui héberge l'instance de Microsoft Exchange Server que vous configurez à des fins de contrôle d'accès. Ouvrez une invite de commande en tant qu'administrateur et exécutez la commande `Winrm quickconfig` . Lorsque l'outil affiche `Effectuer ces`

`modifications [y/n]`, saisissez y. Lorsque la commande aboutit, vous voyez apparaitre le message suivant.

```
WinRM has been updated for remote management.



WinRM service type changed to delayed auto start.

WinRM service started.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this

 machine.
```

1. Ouvrez le Microsoft Exchange Management Shell.
2. Saisissez `New-ManagementRole -Name "<name_new_role_mail_recipients>" -Parent "Mail Recipients"`. Appuyez sur la touche ENTRÉE.
3. Saisissez `New-ManagementRole -Name "<name_new_role_org_ca>" -Parent "Organization Client Access"`. Appuyez sur la touche ENTRÉE.
4. Saisissez `New-ManagementRole -Name "<name_new_role_exchange_servers>" -Parent "Exchange Servers"`. Appuyez sur la touche ENTRÉE.
5. Saisissez `Get-ManagementRoleEntry "<name_new_role_mail_recipients>\*" | Where {$_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry`. Appuyez sur la touche ENTRÉE.
6. Saisissez `Get-ManagementRoleEntry "<name_new_role_org_ca>\*" | Where {$_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry`. Appuyez sur la touche ENTRÉE.
7. Saisissez `Get-ManagementRoleEntry "<name_new_role_exchange_servers>\*" | Where {$_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry`. Appuyez sur la touche ENTRÉE.
8. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox`. Appuyez sur la touche ENTRÉE.
9. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Get-ActiveSyncDevice" -Parameters Identity`. Appuyez sur la touche ENTRÉE.
10. Saisissez `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDeviceStatistics” –Parameters Mailbox`. Appuyez sur la touche ENTRÉE.
11. Saisissez `Add-ManagementRoleEntry “<name_new_role_mail_recipients>\Get-MobileDevice” –Parameters Mailbox`. Appuyez sur la touche ENTRÉE.
12. Saisissez `Add-ManagementRoleEntry "<name_new_role_org_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs`. Appuyez sur la touche ENTRÉE.
13. Saisissez `New-RoleGroup "<name_new_group>" -Roles "<name_new_role_mail_recipients>", "<name_new_role_org_ca>", "<name_new_role_exchange_servers>"`. Appuyez sur la touche ENTRÉE.
14. Saisissez `Add-RoleGroupMember -Identity "<name_new_group>" -Member "BUEMAdmin"`. Appuyez sur la touche ENTRÉE.
15. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Set-AdServerSettings"`. Appuyez sur la touche ENTRÉE.
16. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-ActiveSyncDevice" -Parameters Identity,Confirm`. Appuyez sur la touche ENTRÉE.
17. Saisissez `Add-ManagementRoleEntry "<name_new_role_mail_recipients>\Remove-MobileDevice" -Parameters Identity,Confirm`. Appuyez sur la touche ENTRÉE.

**À la fin :** Autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync.

# Autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync

Si votre entreprise utilise Microsoft Exchange Server, reportez-vous à Configurer Microsoft Exchange pour autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync.

Si votre entreprise utilise Microsoft Office 365, reportez-vous à Configurer la stratégie d'accès des terminaux mobiles dans Microsoft Office 365.

## Configurer Microsoft Exchange pour autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync

Vous devez configurer Microsoft Exchange Server pour autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync. Les terminaux des utilisateurs existants non explicitement ajoutés à la liste autorisée de Microsoft Exchange doivent être mis en quarantaine jusqu'à ce que BlackBerry UEM leur autorise l'accès.

Un seul client de messagerie peut être mis sur liste blanche pour chaque terminal. La priorité pour la liste blanche des applications de messagerie est la suivante :

1. Les applications de messagerie avec une configuration d'application contenant des données de liste blanche du serveur Exchange (uniquement pour Android Enterprise ou Samsung KNOX Play for Work)
2. BlackBerry Work
3. Client de messagerie dans lequel l'ID EAS est envoyé lors de l'inscription

Pour exécuter cette tâche, vous devez être un administrateur Microsoft Exchange disposant des autorisations appropriées pour configurer les paramètres Set-ActiveSyncOrganization. Pour plus d'informations sur la façon d'autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync, rendez-vous sur https://technet.microsoft.com pour consulter l'article *Activer un terminal pour Exchange ActiveSync*.

**Avant de commencer :**

- Configurer des autorisations à des fins de contrôle d'accès.
- Vérifiez auprès de votre administrateur Microsoft Exchange si des utilisateurs utilisent ou non Exchange ActiveSync actuellement.
- Si le niveau d'accès par défaut de votre organisation à Exchange ActiveSync est défini sur Autoriser et que vos utilisateurs sont configurés et synchronisent leurs terminaux avec succès, vous devez vous assurer que ces utilisateurs ont une dispense personnelle ou une règle de terminal associée à leur compte d'utilisateur ou à leur terminal avant de définir le niveau d'accès par défaut sur Quarantaine. Si ce n'est pas le cas, ils sont mis en quarantaine et leurs terminaux ne se synchronisent pas tant qu'ils n'y sont pas autorisés par BlackBerry UEM. Pour plus d'informations sur la définition du niveau d'accès par défaut à Exchange ActiveSync pour la mise en quarantaine, rendez-vous sur support.blackberry.com/community pour consulter l'article 36800.

1. Sur un ordinateur hébergeant Microsoft Exchange Management Shell, ouvrez Microsoft Exchange Management Shell.
2. Saisissez `Set-ActiveSyncOrganizationSettings –DefaultAccessLevel Quarantine`. Appuyez sur la touche ENTRÉE.

**À la fin :** Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès.

## Configurer la stratégie d'accès des terminaux mobiles dans Microsoft Office 365

Pour utiliser BlackBerry Gatekeeping Service avec Microsoft Office 365, vous devez configurer la stratégie d'accès des terminaux mobiles dans Microsoft Office 365 pour la mise en quarantaine de terminaux par défaut.

**Avant de commencer :**

- Configurer des autorisations à des fins de contrôle d'accès.
- Si le niveau d'accès par défaut de votre organisation à Exchange ActiveSync est défini sur Autoriser et que vos utilisateurs sont configurés et synchronisent leurs terminaux avec succès, vous devez vous assurer que ces utilisateurs ont une dispense personnelle ou une règle de terminal associée à leur compte d'utilisateur ou à leur terminal avant de définir le niveau d'accès par défaut sur Quarantaine. Si ce n'est pas le cas, ils sont mis en quarantaine et leurs terminaux ne se synchronisent pas tant qu'ils n'y sont pas autorisés par BlackBerry UEM. Pour plus d'informations sur la configuration du niveau d'accès par défaut de Exchange ActiveSync en quarantaine, rendez-vous sur support.blackberry.com/community pour lire l'article 33531.

1. Connectez-vous au portail d'administration de Microsoft Office 365.
2. Dans le menu latéral, cliquez sur **Admin**.
3. Cliquez sur **Exchange**.
4. Dans la section **Mobile**, cliquez sur **Accès des terminaux mobiles**.
5. Cliquez sur **Modifier**.
6. Cliquez sur **Quarantaine - Me laisser décider de bloquer ou d'autoriser plus tard**.

**À la fin :** Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès.

# Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès

BlackBerry UEM utilise les commandes Windows PowerShell pour gérer la liste des terminaux autorisés. Pour utiliser BlackBerry Gatekeeping Service, vous devez configurer les autorisations Microsoft IIS. Procédez comme suit sur l'ordinateur qui héberge le rôle de serveur d'accès client Microsoft.

**Avant de commencer :** Autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync.

1. Ouvrez Microsoft Internet Information Services (IIS) Manager.
2. Dans le volet de gauche, développez le serveur.
3. Développez **Sites** > **Site Web par défaut**.
4. Cliquez avec le bouton droit sur le dossier PowerShell. Sélectionnez **Modifier les autorisations**.
5. Cliquez sur l'onglet **Sécurité**. Cliquez sur **Modifier**.
6. Cliquez sur **Ajouter** et saisissez le <nouveau_groupe> créé lors de la configuration des autorisations Microsoft Exchange à des fins de contrôle d'accès.
7. Cliquez sur **OK**.
8. Vérifiez que les paramètres **Lecture et exécution**, **Affichage du contenu du dossier** et **Lecture** sont sélectionnés. Cliquez sur **OK**.
9. Sélectionnez le dossier **PowerShell**. Double-cliquez sur l'icône **Authentification**.
10. Sélectionnez **Authentification Windows**. Cliquez sur **Activer**.
11. Fermez Microsoft Internet Information Services (IIS) Manager.

**À la fin :** Créer une configuration de contrôle d'accès.

# Ajouter une application et obtenir des détails Azure pour configurer l'authentification moderne

Lorsque vous configurez l'authentification moderne, vous devez fournir deux détails de l'application : l'ID d'application et l'organisation.

1. Connectez-vous à portal.azure.com.
2. Cliquez sur **App registrations**.
3. Cliquez sur **Nouvelle inscription**.
4. Dans le champ **Nom**, saisissez un nom pour l'application.
5. Cliquez sur **S'inscrire**.
6. Cliquez sur **Autorisations API > Ajouter une autorisation**.
7. Recherchez le groupe d'autorisations **Exchange** ou **Office 365 Exchange Online**.
8. Cliquez sur **Autorisations d'application > Exchange.ManageAsApp > Ajouter une autorisation**.
9. Pour accorder le consentement de l'administrateur, sélectionnez **Exchange.ManageAsApp > Accorder le consentement de l'administrateur**.
10. Dans la section Gérer, cliquez sur **Certificats et secrets > Télécharger le certificat** et sélectionnez la clé publique (cert.pem)
11. Pour attribuer un rôle à l'application, sur la page d'accueil Azure, cliquez sur **Azure Active Directory**.
12. Cliquez sur **Rôles et administrateurs**.
13. Dans la section **Rôles administratifs**, saisissez Exchange pour afficher les rôles pris en charge pour Microsoft Exchange.
14. Cliquez sur un rôle pour afficher les détails du rôle.
15. Cliquez sur **Ajouter des attributions**.
16. Sous **Sélectionner un ou plusieurs membres**, cliquez sur **Aucun membre sélectionné**.
17. Recherchez l'ID d'application Azure par ID ou nom de l'application.
18. Sélectionnez l'application que vous avez créée précédemment pour la déplacer dans la section **Éléments sélectionnés**.
19. Cliquez sur **Sélectionner**.

    L'ID d'application Azure s'affiche désormais dans la section **Sélectionner un ou plusieurs membres**. Les informations sur l'organisation Azure s'affichent sur la page Azure Active Directory en tant que propriété du répertoire. Enregistrez ces deux entrées pour les utiliser lorsque vous configurez BlackBerry UEM pour l'authentification moderne.
20. Cliquez sur **Suivant**.
21. Sur la page **Ajouter des attributions**, assurez-vous que le **type d'attribution** est défini sur **Actif**. Pour plus d'informations sur les types d'attribution, reportez-vous aux informations de Microsoft.
22. Cliquez sur **Attribuer**.

**À la fin :** Créer une configuration de contrôle d'accès

# Associer un certificat avec l'ID d'application Azure pour UEM

Vous pouvez demander et exporter un nouveau certificat client depuis votre serveur CA ou utiliser un certificat auto-signé. La clé privée doit être au format .pfx. La clé publique peut être exportée en tant que fichier .cer ou .pem à télécharger sur Microsoft Azure.

1. Effectuez l'une des tâches suivantes :

| Certificat | Tâche |
| --- | --- |

| | |
|---|---|
| Si vous utilisez un serveur CA existant | **a.** Demandez le certificat. Le certificat que vous demandez doit inclure le nom de l'application dans l'objet du certificat. <*nom de l'application*> est le nom que vous avez attribué à l'application à l'étape 4 de la section Ajouter une application et obtenir des détails Azure pour configurer une authentification moderne.<br>**b.** Exportez la clé publique du certificat en tant que fichier .cer ou .pem. La clé publique est utilisée pour l'ID d'application Azure qui est créé.<br>**c.** Exportez la clé privée du certificat en tant que fichier .pfx. |

| | |
|---|---|
| Si vous utilisez un certificat auto-signé | **a.** Créez un certificat auto-signé à l'aide de la commande New-SelfSignedCertificate. Pour plus d'informations, visitez le site docs.microsoft.com et lisez le contenu relatif à la commande New-SelfSignedCertificate.<br>**1.** Sur l'ordinateur exécutant Microsoft Windows, ouvrez Windows PowerShell.<br>**2.** Saisissez la commande suivante : `$cert=New-SelfSignedCertificate -Subject "CN=<nom de l'application>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`. <*nom de l'application*> est le nom que vous avez attribué à l'application à l'étape 4 de la section Ajouter une application et obtenir des détails Azure pour configurer une authentification moderne. Le certificat que vous demandez doit inclure le nom de l'application Azure dans le champ objet.<br>**3.** Appuyez sur la touche **Entrée**.<br>**b.** Exportez la clé publique à partir de Microsoft Management Console (MMC). Assurez-vous de sauvegarder le certificat public en tant que fichier .cer ou .pem. La clé publique est utilisée pour l'ID d'application Azure qui est créé.<br>**1.** Sur l'ordinateur exécutant Windows, ouvrez le gestionnaire de certificats pour l'utilisateur connecté.<br>**2.** Développez **Personnel**.<br>**3.** Cliquez sur **Certificats**.<br>**4.** Cliquez avec le bouton droit sur <*utilisateur*>@<*domaine*, puis cliquez sur **Toutes les tâches > Exporter**.<br>**5.** Dans l'**Assistant d'exportation de certificat**, cliquez sur **Non, ne pas exporter la clé privée**.<br>**6.** Cliquez sur **Suivant**.<br>**7.** Sélectionnez **Base-64 encoded X.509 (.cer)**. Cliquez sur **Suivant**.<br>**8.** Donnez un nom au certificat et enregistrez-le sur votre bureau.<br>**9.** Cliquez sur **Suivant**.<br>**10.** Cliquez sur **Terminer**.<br>**11.** Cliquez sur **OK**.<br>**c.** Exportez la clé privée à partir de Microsoft Management Console (MMC). Assurez-vous d'inclure la clé privée et de la sauvegarder en tant que fichier .pfx. Pour obtenir des instructions, visitez le site docs.microsoft.com et lisez le document Exporter un certificat avec la clé privée.<br>**1.** Sur l'ordinateur exécutant Windows, ouvrez le gestionnaire de certificats pour l'utilisateur connecté.<br>**2.** Développez **Personnel**.<br>**3.** Cliquez sur **Certificats**.<br>**4.** Cliquez avec le bouton droit sur <*utilisateur*>@<*domaine*, puis cliquez sur **Toutes les tâches > Exporter**.<br>**5.** Dans l'**Assistant d'exportation de certificat**, cliquez sur **Oui, exporter la clé privée.**.<br>**6.** Cliquez sur **Suivant**.<br>**7.** Sélectionnez **Échange d'informations personnelles – PKCS #12 (.pfx)**. Cliquez sur **Suivant**.<br>**8.** Sélectionnez la méthode de sécurité.<br>**9.** Donnez un nom au certificat et enregistrez-le sur votre bureau.<br>**10.** Cliquez sur **Suivant**.<br>**11.** Cliquez sur **Terminer**.<br>**12.** Cliquez sur **OK**. |

2. Téléchargez le certificat public (fichier .pem ou .cer) que vous avez exporté à l'étape 1 pour associer les informations d'identification du certificat à l'ID de l'application Azure pour UEM.
   a) Sur portal.azure.com, ouvrez le <*nom de l'application*> que vous avez attribué à l'application à l'étape 4 de la section Ajouter une application et obtenir des détails Azure pour configurer l'authentification moderne.
   b) Cliquez sur **Certificats & secrets**.
   c) Dans la section **Certificat**, cliquez sur **Charger le certificat**.
   d) Dans le champ de recherche **Sélectionner un fichier**, accédez à l'emplacement où vous avez exporté le certificat.
   e) Cliquez sur **Ajouter**.

# Créer une configuration de contrôle d'accès

Vous pouvez créer une configuration de contrôle d'accès permettant aux terminaux conformes aux stratégies de sécurité de votre entreprise de se connecter à Microsoft Exchange Server ou Microsoft Office 365.

**Avant de commencer :**

- Configurer des autorisations à des fins de contrôle d'accès.
- Autoriser uniquement les terminaux approuvés à accéder à Exchange ActiveSync.
- Configurer les autorisations Microsoft IIS à des fins de contrôle d'accès.
- Ajouter une application et obtenez des détails Azure pour configurer l'authentification moderne.

1. Effectuez l'une des opérations suivantes :
   - Si vous disposez de BlackBerry UEM dans un environnement sur site, dans la barre de menus, cliquez sur **Paramètres > Intégration externe > Service de contrôle Microsoft Exchange**.
   - Si vous disposez de BlackBerry UEM Cloud, dans la console BlackBerry Connectivity Node (http:/localhost:8088), cliquez sur **Paramètres généraux > BlackBerry Gatekeeping Service**.
2. Dans la section Liste Microsoft Exchange Server, cliquez sur +.
3. Effectuez l'une des tâches suivantes :

| Tâche | Étapes |
|---|---|
| Se connecter à Microsoft Office 365 à l'aide de l'authentification moderne | Avant de configurer BlackBerry UEM pour utiliser l'authentification moderne, vous devez générer un certificat contenant des clés publique et privée. Vous pouvez utiliser OpenSSL ou PowerShell pour générer le certificat.<br>**a.** Cochez la case **Authentification moderne**.<br>**b.** Dans le champ **Nom de connexion Exchange Online**, saisissez un nom de connexion.<br>**c.** Cliquez sur **Parcourir** et sélectionnez le certificat à utiliser pour l'authentification.<br>**d.** Dans le champ **Mot de passe du certificat**, saisissez le mot de passe du certificat.<br>**e.** Spécifiez votre **ID d'application Azure**.<br>**f.** Renseignez le champ **Organisation Azure**. |

| Tâche | Étapes |
| --- | --- |
| Se connecter à Microsoft Exchange Server ou Microsoft Office 365 à l'aide de l'authentification de base | a. Dans le champ **Nom du serveur**, saisissez le nom de l'environnement Microsoft Exchange Server ou Microsoft Office 365 dont vous souhaitez gérer l'accès.<br>b. Saisissez le nom d'utilisateur et le mot de passe du compte que vous avez créé pour gérer le contrôle d'accès de Exchange ActiveSync.<br>c. Dans la liste déroulante **Type d'authentification**, sélectionnez le type d'authentification utilisé pour Microsoft Exchange Server ou Microsoft Office 365.<br>d. Dans la liste déroulante **Type d'authentification**, sélectionnez le type d'authentification utilisé pour Microsoft Exchange Server ou Microsoft Office 365.<br>e. Pour activer l'authentification SSL entre BlackBerry UEM et Microsoft Exchange Server ou Microsoft Office 365, cochez la case **Utiliser SSL**. Vous pouvez également sélectionner d'autres contrôles de certificats.<br>f. Dans la liste déroulante **Type de proxy**, sélectionnez le type de configuration proxy utilisé entre BlackBerry UEM et Microsoft Exchange Server ou Microsoft Office 365, le cas échéant.<br>g. Si vous avez sélectionné une configuration proxy à l'étape précédente, sélectionnez le type d'authentification utilisé sur le serveur proxy.<br>h. Si nécessaire, sélectionnez **Authentification requise** et saisissez le nom d'utilisateur et le mot de passe. |

4. Cliquez sur **Test de connexion** pour vérifier que la connexion a abouti.
5. Cliquez sur **Enregistrer**.

**À la fin :**

- Créer un profil de contrôle d'accès et attribuez-le aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.
- Si vous avez configuré un groupe de serveurs avec une ou plusieurs instances actives de BlackBerry Gatekeeping Service, associez le profil de contrôle d'accès au groupe de serveurs approprié. Tout utilisateur auquel est attribué ce profil de contrôle d'accès peut utiliser n'importe quelle instance active de BlackBerry Gatekeeping Service dans ce groupe de serveurs.

# Créer un profil de contrôle d'accès

Si vous utilisez le contrôle d'accès automatique, créez un profil de contrôle d'accès.

Si vous configurez BlackBerry Gatekeeping Service, vous devez créer un profil de contrôle d'accès et l'attribuer aux comptes d'utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux. Le profil de contrôle d'accès vous permet de sélectionner les serveurs Microsoft Exchange pour un contrôle d'accès automatique.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > Contrôle**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Cliquez sur **Sélectionner des serveurs**.
6. Sélectionnez un ou plusieurs serveurs, puis cliquez sur →.

7. Cliquez sur **Enregistrer**.

# Vérification qu'un terminal est autorisé à accéder à la messagerie professionnelle et aux données de l'organiseur

Lorsque votre organisation utilise BlackBerry Gatekeeping Service pour contrôler les terminaux qui peuvent accéder à la messagerie professionnelle et aux données de l'organiseur depuis Exchange ActiveSync, au moins un serveur de contrôle d'accès est configuré sur un profil de messagerie. Lorsque le profil de messagerie avec contrôle d'accès configuré est attribué à un compte d'utilisateur, vous pouvez vérifier l'état de la connexion entre un terminal et Exchange ActiveSync. Vous pouvez localiser cet état en consultant la page des détails du terminal de la section Stratégie informatique et profils. Les états suivants s'affichent dans les détails du terminal en regard du profil de messagerie.

| État | Description |
|---|---|
| Inconnu | L'état Inconnu s'affiche lorsque BlackBerry UEM ne peut pas déterminer l'ID du terminal. Le terminal est répertorié dans la liste limitée des terminaux et doit être manuellement ajouté à la liste autorisée. |
| Connexion en attente | L'état Connexion en attente s'affiche lorsque BlackBerry UEM connait l'ID du terminal et que le terminal est mis en file d'attente pour être ajouté à la liste autorisée. |
| Connexion autorisée | L'état Connexion autorisée s'affiche lorsque BlackBerry UEM connait l'ID du terminal et que le terminal se trouve sur la liste autorisée. |

### Vérifier qu'un terminal est autorisé à accéder à Exchange ActiveSync

1. Sur la barre de menus, cliquez sur **Utilisateurs > Terminaux gérés**.
2. Recherchez un compte d'utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom d'un compte d'utilisateur.
4. Sélectionnez l'onglet correspondant au terminal que vous souhaitez vérifier.
5. Dans la section **Stratégie informatique et profils**, si le terminal est autorisé, **Connexion autorisée** s'affiche en regard du profil de messagerie.

# Autoriser un terminal à accéder à Microsoft ActiveSync

Si BlackBerry UEM ne parvient pas à obtenir l'ID Exchange ActiveSync d'un terminal, celui-ci n'est pas ajouté à la liste autorisée pour Microsoft Exchange. Vous pouvez ajouter manuellement ces terminaux à la liste autorisée depuis la liste des terminaux Exchange ActiveSync limités. Par exemple, si un terminal Android est activé via le type d'activation MDM, BlackBerry UEM n'est alors pas en mesure d'obtenir un ID Exchange ActiveSync et vous devez autoriser manuellement le terminal dans la liste des terminaux Exchange ActiveSync limités.

1. Sur la barre de menus, cliquez sur **Utilisateurs > Exchange Gatekeeping**.
2. Recherchez un terminal.
3. Dans la colonne **Action**, cliquez sur ✓.

# Bloquer l'accès d'un terminal à Microsoft ActiveSync

Vous pouvez bloquer manuellement l'accès d'un terminal précédemment autorisé à Microsoft ActiveSync. Ce faisant, le terminal empêche l'utilisateur de récupérer des e-mails et d'autres informations depuis Microsoft Exchange Server sur le terminal.

1. Sur la barre de menus, cliquez sur **Utilisateurs**.
2. Cliquez sur **Service de contrôle Exchange**.
3. Recherchez un terminal.
4. Dans la colonne **Action**, cliquez sur ⃠.

# Créer des profils de messagerie

Vous pouvez utiliser les profils de messagerie pour spécifier la manière dont les terminaux se connectent au serveur de messagerie de votre organisation et synchronisent les e-mails, les entrées de calendrier et les données de l'organiseur à l'aide de Exchange ActiveSync ou IBM Notes Traveler.

Vous n'avez pas besoin d'utiliser un profil de messagerie si votre organisation utilise BlackBerry Work pour gérer les e-mails, le calendrier et les contacts des terminaux des utilisateurs. Pour plus d'informations sur la gestion de BlackBerry Work, consultez la section Gestion des applications BlackBerry Dynamics et le Guide d'administration de BlackBerry Work.

Si vous souhaitez utiliser Exchange ActiveSync, notez ce qui suit :

- Pour une sécurité renforcée de la messagerie, vous pouvez activer S/MIME pour les terminaux iOS et Android.
- Si vous activez S/MIME, vous pouvez utiliser d'autres profils pour permettre aux terminaux de récupérer automatiquement des certificats S/MIME et en vérifier l'état.

Si vous souhaitez utiliser Notes Traveler, notez ce qui suit :

- Pour utiliser Notes Traveler avec les terminaux iOS, vous devez activer BlackBerry Secure Gateway.

Vous pouvez également utiliser les profils de messagerie IMAP/POP3 pour spécifier la manière dont les terminaux iOS, macOS, Android et Windows se connectent aux serveurs de messagerie IMAP ou POP3 et synchronisent les e-mails. Les terminaux activés pour utiliser Knox MDM ne prennent pas en charge les protocoles IMAP ou POP3.

# Créer un profil de messagerie

Les paramètres de profil requis varient pour chaque type de terminal et dépendent du serveur de messagerie dans l'environnement de votre entreprise.

**Avant de commencer :**

- Si vous utilisez l'authentification basée sur des certificats entre les terminaux et le serveur de messagerie, vous devez créer un profil de certificat d'autorité de certification et l'attribuer aux utilisateurs. Vous devez également veiller à ce que les terminaux disposent d'un certificat client approuvé.
- Pour les terminaux Android avec des activations Contrôles MDM, BlackBerry UEM envoie le profil de messagerie aux terminaux, mais l'utilisateur doit configurer manuellement la connexion au serveur de messagerie.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > E-mail**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Si nécessaire, saisissez le nom de domaine du serveur de messagerie. Si le profil concerne plusieurs utilisateurs pouvant se trouver dans différents domaines Microsoft Active Directory, vous pouvez utiliser la variable `%UserDomain%`.
6. Dans le champ **Adresse électronique**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un utilisateur, saisissez l'adresse électronique de l'utilisateur.
   - Si le profil correspond à plusieurs utilisateurs, saisissez `%UserEmailAddress%`.
7. Saisissez le nom d'hôte ou l'adresse IP du serveur de messagerie.
8. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :

- Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.
- Si le profil correspond à plusieurs utilisateurs, saisissez `%UserName%`.
- Si le profil concerne plusieurs utilisateurs dans un environnement IBM Notes Traveler, saisissez `%UserDisplayName%`.

9. Si vous avez configuré des groupes de serveurs pour diriger le trafic BlackBerry Secure Gateway vers une connexion régionale spécifique de BlackBerry Infrastructure, cliquez sur le groupe de serveurs approprié dans la liste déroulante **Groupe de serveurs BlackBerry Secure Gateway Service**.

   Pour plus d'informations sur BlackBerry Connectivity Node et les groupes de serveurs, reportez-vous au contenu relatif à la planification et au contenu relatif à l'installation et à la mise à niveau ou le contenu relatif à la configuration de UEM Cloud
10. Cliquez sur l'onglet correspondant à chaque type de terminal de votre organisation et configurez les valeurs appropriées pour chaque paramètre de profil.
11. Cliquez sur **Ajouter**.

**À la fin :** Si nécessaire, classez les profils.

# Paramètres de profil de messagerie

Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle. Les profils de messagerie sont pris en charge sur les types de terminaux suivants :

- iOS
- macOS
- Android
- Windows

### Commun : Paramètres de profil de messagerie

| Commun : paramètre Profil de messagerie | Description |
|---|---|
| Nom de domaine | Ce paramètre spécifie le nom de domaine du serveur de messagerie. |
| Adresse électronique | Ce paramètre spécifie l'adresse électronique de l'utilisateur. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserEmailAddress%. |
| Nom d'hôte ou adresse IP | Ce paramètre spécifie le nom d'hôte ou l'adresse IP du serveur de messagerie. |
| nom d'utilisateur ; | Ce paramètre spécifie le nom d'utilisateur de l'utilisateur. Si le profil concerne plusieurs utilisateurs, vous pouvez utiliser la variable %UserName%. |

| Commun : paramètre Profil de messagerie | Description |
|---|---|
| Serveurs de contrôle d'accès automatique | Si vous avez configuré des groupes de serveurs pour diriger le trafic BlackBerry Secure Gateway ou BlackBerry Gatekeeping Service vers une connexion régionale spécifique à BlackBerry Infrastructure, ce paramètre spécifie le groupe de serveurs approprié.<br><br>Pour obtenir plus d'informations sur BlackBerry Connectivity Node et les groupes de serveurs dans un environnement sur site, reportez-vous au contenu relatif à la planification et au contenu relatif à l'installation et à la mise à niveau. Pour obtenir plus d'informations sur BlackBerry Connectivity Node et les groupes de serveurs dans un environnement Cloud, consultez le contenu relatif à la configuration BlackBerry UEM Cloud. |

## iOS : paramètres de profil de messagerie

Ces paramètres s'appliquent également aux terminaux iPadOS

| iOS : paramètre de profil de messagerie | Description |
|---|---|
| **Paramètres de remise** | |
| Autoriser le déplacement de messages | Ce paramètre spécifie si les utilisateurs peuvent déplacer les e-mails de ce compte vers un autre compte de messagerie présent sur un terminal. |
| Autoriser la synchronisation des adresses récentes | Ce paramètre spécifie si un utilisateur peut synchroniser les adresses récemment utilisées sur les terminaux. |
| Utiliser uniquement dans la messagerie | Ce paramètre spécifie si les applications autres que l'application de messagerie peuvent utiliser ce compte pour envoyer des e-mails. |
| Activer S/MIME | Ce paramètre spécifie si un utilisateur peut envoyer des e-mails protégés par S/MIME. |
| Activer messages S/MIME signés numériquement | Ce paramètre spécifie si un terminal envoie des messages sortants avec une signature numérique.<br><br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |

| iOS : paramètre de profil de messagerie | Description |
| --- | --- |
| Informations d'identification de signature | Ce paramètre spécifie la manière dont les terminaux trouvent les certificats requis pour signer les messages.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.<br>Valeurs possibles :<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>Après avoir choisi le type de profil que vous souhaitez utiliser, spécifiez le profil de certificat partagé, profil SCEP ou profil des informations d'identification de l'utilisateur.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| Certificat partagé de signature | Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de signer des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| SCEP de signature | Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis pour signer les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| Informations d'identification de connexion de l'utilisateur | Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour obtenir les certificats client requis pour signer les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| L'utilisateur peut activer ou désactiver la signature S/MIME | Ce paramètre spécifie si un utilisateur est autorisé à activer ou désactiver la signature S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| L'utilisateur peut changer les identifiants de signature | Ce paramètre spécifie si un utilisateur peut remplacer les identifiants de signature.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| Activer le cryptage des messages S/MIME | Ce paramètre spécifie si un terminal crypte les e-mails sortants à l'aide du cryptage S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |

| iOS : paramètre de profil de messagerie | Description |
| --- | --- |
| Informations d'identification de cryptage | Ce paramètre spécifie la manière dont les terminaux trouvent les certificats requis pour crypter les messages.<br>Valeurs possibles :<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>Après avoir sélectionné le type de profil, sélectionnez le profil de certificat partagé, profil SCEP ou profil des informations d'identification de l'utilisateur que vous souhaitez utiliser.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| Certificat partagé de cryptage | Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de crypter des e-mails.<br>Les terminaux choisissent le certificat adapté au destinataire pour crypter les messages à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| SCEP de cryptage | Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis et crypter les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| Informations d'identification de l'utilisateur de cryptage | Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour récupérer les certificats client requis et crypter les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| L'utilisateur peut remplacer le cryptage S/MIME | Ce paramètre spécifie si un utilisateur peut activer ou désactiver le paramètre de cryptage.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| L'utilisateur peut remplacer les identifiants de cryptage S/MIME | Ce paramètre spécifie si un utilisateur peut remplacer les identifiants de cryptage S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |

| iOS : paramètre de profil de messagerie | Description |
|---|---|
| Crypter les messages | Ce paramètre spécifie si tous les e-mails doivent être cryptés lorsque l'utilisateur les envoie (Obligatoire) ou si l'utilisateur peut choisir les messages à crypter au moment où il les envoie (Autoriser).<br>Ce paramètre s'applique uniquement si le paramètre Activer S/MIME est sélectionné.<br>Valeurs possibles :<br>• Requise<br>• Autoriser<br>La valeur par défaut est Requis.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné. |
| Jours de synchronisation | Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal.<br>Valeurs possibles :<br>• 1 jour<br>• 3 jours<br>• 7 jours<br>• 14 jours<br>• 1 mois<br>• Toujours<br>La valeur par défaut est 7 jours.<br>**Remarque :** Ce paramètre s'applique uniquement aux applications de messagerie et de l'organiseur par défaut des terminaux avec le type d'activation Contrôles MDM. |
| VPN par compte | Ce paramètre spécifie le profil VPN utilisé pour la communication réseau de ce compte. Ce paramètre s'applique uniquement aux terminaux iOS 14 ou version ultérieure, et iPadOS 14 ou version ultérieure. |
| **Authentification** | |
| Activer BlackBerry Secure Gateway | Ce paramètre spécifie si les terminaux utilisant le type d'activation Contrôles MDM utilisent BlackBerry Secure Gateway pour se connecter au serveur de messagerie. BlackBerry Secure Gateway fournit une connexion sécurisée au serveur de messagerie de votre organisation via BlackBerry Infrastructure et BlackBerry UEM.<br>Si vous avez configuré des groupes de serveurs de manière à rediriger le trafic BlackBerry Secure Gateway vers une connexion locale spécifique à BlackBerry Infrastructure, vous devez associer le profil de messagerie au groupe de serveurs approprié. |

| iOS : paramètre de profil de messagerie | Description |
| --- | --- |
| Type d'authentification | Ce paramètre spécifie le type d'authentification utilisé par un terminal pour se connecter au serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné.<br>Valeurs possibles :<br>• Aucun<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>La valeur par défaut est Aucune. |
| Profil de certificat partagé | Ce paramètre spécifie le profil de certificat partagé du certificat client utilisé par un terminal pour se connecter au serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Type d'authentification ou le paramètre Méthode d'authentification est défini sur Certificat partagé. |
| Profil SCEP associé | Ce paramètre spécifie le profil SCEP associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné et si le paramètre Type d'authentification est défini sur SCEP. |
| Profil des informations d'identification de l'utilisateur associé | Ce paramètre spécifie le profil des informations d'identification de l'utilisateur associé utilisé par un terminal pour obtenir un certificat client et s'authentifier auprès du serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné et si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur. |
| Utiliser des informations d'identification et un certificat | Ce paramètre spécifie si un terminal utilise des informations d'identification et un certificat client obtenus à l'aide du profil SCEP associé pour s'authentifier auprès du serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné et si le paramètre Type d'authentification est défini sur SCEP. |
| Utiliser OAuth pour l'authentification | Ce paramètre indique si la connexion doit utiliser OAuth pour l'authentification. |
| URL de connexion OAuth | Ce paramètre spécifie l'URL que ce compte doit utiliser pour se connecter à OAuth. Lorsque vous spécifiez cette URL, vous devez indiquer un hôte car la détection automatique n'est pas utilisée.<br>Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné. |

| iOS : paramètre de profil de messagerie | Description |
| --- | --- |
| URL de demande de jeton OAuth | Ce paramètre spécifie l'URL que ce compte doit utiliser pour les demandes de jeton utilisant OAuth<br>Ce paramètre est valide uniquement si le paramètre Activer BlackBerry Secure Gateway n'est pas sélectionné. |
| Utiliser SSL | Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie. |
| Accepter tous les certificats SSL | Ce paramètre indique si tous les certificats SSL sont acceptés.<br>Ce paramètre est valide uniquement si le paramètre Utiliser SSL est sélectionné. |
| **Domaines de messagerie externes** | |
| Liste autorisée des domaines de messagerie externes | Ce paramètre spécifie la liste de domaines vers lesquels un utilisateur peut envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, lorsqu'un utilisateur ajoute un destinataire disposant d'une adresse électronique dans le domaine autorisé à un e-mail ou une entrée de calendrier, aucun message d'avertissement ne s'affiche. Ce paramètre s'applique à l'espace Travail uniquement.<br>Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace. |
| Liste restreinte des domaines de messagerie externes | Ce paramètre spécifie la liste de domaines vers lesquels les utilisateurs peuvent envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, si un utilisateur tente d'ajouter un destinataire disposant d'une adresse électronique correspondant au domaine limité à un e-mail ou une invitation de calendrier, l'application Work Connect ne permet pas à l'utilisateur de mener à bien cette opération. Ce paramètre s'applique à l'espace Travail uniquement.<br>Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace. |
| **Services activés** | |
| Messagerie | Ce paramètre indique si les utilisateurs peuvent accéder à leur messagerie professionnelle sur le terminal. |
| Contacts | Ce paramètre indique si les utilisateurs peuvent accéder à leurs contacts professionnels sur le terminal. |
| Calendriers | Ce paramètre indique si les utilisateurs peuvent accéder à leur calendrier professionnel sur le terminal. |
| Rappels | Ce paramètre indique si les utilisateurs peuvent accéder à leurs rappels professionnels sur le terminal. |
| Notes | Ce paramètre indique si les utilisateurs peuvent accéder à leurs notes de travail sur le terminal. |

| iOS : paramètre de profil de messagerie | Description |
|---|---|
| **Modification du compte** | |
| Messagerie | Ce paramètre indique si les utilisateurs peuvent modifier l'activation ou la désactivation de la messagerie professionnelle sur le terminal. |
| Contacts | Ce paramètre indique si les utilisateurs peuvent modifier l'activation ou la désactivation de l'accès aux contacts professionnels sur le terminal. |
| Calendriers | Ce paramètre indique si les utilisateurs peuvent modifier l'activation ou la désactivation de l'accès à leur calendrier professionnel sur le terminal. |
| Rappels | Ce paramètre indique si les utilisateurs peuvent modifier l'activation ou la désactivation de l'accès à leurs rappels professionnels sur le terminal. |
| Notes | Ce paramètre indique si les utilisateurs peuvent modifier l'activation ou la désactivation de l'accès à leurs notes de travail sur le terminal. |

### macOS : paramètres de profil de messagerie

macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils de messagerie électronique sont appliqués aux comptes d'utilisateur.

| macOS : paramètre de profil de messagerie | Description |
|---|---|
| Chemin d'accès | Ce paramètre spécifie le chemin de réseau du serveur de messagerie. |
| Port | Ce paramètre spécifie le port utilisé pour se connecter au serveur de messagerie. |
| Utiliser SSL | Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie. |
| Nom d'hôte ou adresse IP externe | Ce paramètre spécifie le nom d'hôte ou l'adresse IP externe du serveur de messagerie. |
| Utiliser un protocole SSL externe | Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie externe. |
| Chemin d'accès externe | Ce paramètre spécifie le chemin de réseau du serveur de messagerie externe. |
| Port du serveur externe | Ce paramètre spécifie le port utilisé pour se connecter au serveur de messagerie externe. |

## Android : Paramètres de profil de messagerie

| Android : Paramètre de profil de messagerie | Description |
|---|---|
| **Paramètres de remise** | |
| Type de profil | Ce paramètre spécifie si vous souhaitez que ce profil prenne en charge Exchange ActiveSync ou IBM Notes Traveler.<br>Valeurs possibles :<br>• Exchange ActiveSync<br>• IBM Notes Traveler<br>La valeur par défaut est Exchange ActiveSync. |
| Jours de synchronisation | Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et les données de l'organiseur avec un terminal Android doté du type d'activation Contrôles MDM.<br>Valeurs possibles :<br>• Illimité<br>• 1 jour<br>• 3 jours<br>• 7 jours<br>• 14 jours<br>• 1 mois<br>La valeur par défaut est de 1 mois.<br>Pour les terminaux Android utilisant Samsung Knox MDM, si vous définissez la valeur sur Illimité, un seul mois est synchronisé.<br>**Remarque :** Ce paramètre s'applique uniquement aux applications de messagerie et de l'organiseur par défaut des terminaux Android avec le type d'activation Contrôles MDM. |
| Type d'authentification | Ce paramètre spécifie le type d'authentification utilisé par un terminal Android pour se connecter au serveur de messagerie.<br>Valeurs possibles :<br>• Aucun<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>La valeur par défaut est Aucune. |
| Profil SCEP associé | Ce paramètre spécifie le profil SCEP associé utilisé par un terminal Android pour obtenir un certificat client et s'authentifier auprès du serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP. |

| Android : Paramètre de profil de messagerie | Description |
| --- | --- |
| Utiliser des informations d'identification et un certificat | Ce paramètre spécifie si un terminal utilise des informations d'identification et un certificat client obtenus à l'aide du profil SCEP associé pour s'authentifier auprès du serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur SCEP. |
| Profil de certificat partagé | Ce paramètre spécifie le profil de certificat partagé du certificat client utilisé par un terminal Android pour se connecter au serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Certificat partagé. |
| Profil des informations d'identification de l'utilisateur associé | Ce paramètre spécifie le profil des informations d'identification de l'utilisateur du certificat client utilisé par un terminal Android pour se connecter au serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Type d'authentification est défini sur Informations d'identification de l'utilisateur. |
| Utiliser SSL | Ce paramètre spécifie si un terminal doit utiliser SSL pour se connecter au serveur de messagerie. |
| Accepter tous les certificats SSL | Ce paramètre spécifie si un terminal doit accepter automatiquement les certificats SSL non approuvés du serveur de messagerie. S'il n'est pas sélectionné, les terminaux peuvent se connecter uniquement aux serveurs de messagerie qui utilisent un certificat SSL approuvé. |
| Taille maximale des pièces jointes aux e-mails | Ce paramètre spécifie la taille maximale autorisée pour les pièces jointes d'e-mail (en Mo).<br>Les valeurs possibles sont 1 à 365. Le paramètre par défaut est 25.<br>Ce paramètre s'applique uniquement aux terminaux Android Enterprise. |
| Signature électronique par défaut pour les nouveaux messages | Ce paramètre spécifie une signature d'e-mail qui est automatiquement ajoutée aux nouveaux e-mails.<br>Ce paramètre s'applique uniquement aux terminaux Android Enterprise. |
| Activer S/MIME | Ce paramètre spécifie si les terminaux peuvent envoyer des e-mails protégés par S/MIME.<br>Pour les terminaux qui utilisent BlackBerry Productivity Suite, vous devez définir une valeur pour le paramètre Prise en charge S/MIME. |

| Android : Paramètre de profil de messagerie | Description |
| --- | --- |
| Signer les messages | Ce paramètre spécifie si les terminaux envoient tous les e-mails sortants avec une signature numérique.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.<br>Pour les terminaux Android Enterprise, ce paramètre s'applique uniquement aux terminaux qui utilisent Divide Productivity.<br>Pour les terminaux qui utilisent BlackBerry Productivity Suite, vous devez définir une valeur pour le paramètre Messages S/MIME signés numériquement. |
| Informations d'identification de signature | Ce paramètre spécifie les identifiants que le terminal utilisera pour signer les e-mails.<br>Ce paramètre est valide uniquement si le paramètre Signer les messages est sélectionné.<br>Valeurs possibles :<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>La valeur par défaut est Certificat partagé. |
| Certificat partagé de signature | Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de signer des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Certificat partagé. |
| SCEP de signature | Ce paramètre spécifie le profil SCEP pour un certificat client utilisé par un terminal afin de signer des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur SCEP. |
| Informations d'identification de connexion de l'utilisateur | Ce paramètre spécifie le profil d'identifiants de connexion pour un certificat client utilisé par un terminal afin de signer des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Identifiants de connexion d'utilisateur. |
| Crypter les messages | Ce paramètre spécifie si les terminaux cryptent les e-mails sortants à l'aide du cryptage S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.<br>Pour les terminaux Android Enterprise, ce paramètre s'applique uniquement aux terminaux qui utilisent Divide Productivity.<br>Pour les terminaux qui utilisent BlackBerry Productivity Suite, vous devez définir une valeur pour le paramètre Messages S/MIME signés numériquement. |

| Android : Paramètre de profil de messagerie | Description |
|---|---|
| Informations d'identification de cryptage | Ce paramètre spécifie les identifiants que le terminal utilisera pour crypter les e-mails.<br>Ce paramètre est valide uniquement si le paramètre Crypter les messages est sélectionné.<br>Valeurs possibles :<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>La valeur par défaut est Certificat partagé. |
| Certificat partagé de cryptage | Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de crypter des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur Certificat partagé. |
| SCEP de cryptage | Ce paramètre spécifie le profil SCEP pour un certificat client utilisé par un terminal afin de crypter des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur SCEP. |
| Informations d'identification de l'utilisateur de cryptage | Ce paramètre spécifie le profil d'identifiants de connexion pour un certificat client utilisé par un terminal afin de crypter des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Identifiants de connexion d'utilisateur. |
| Exiger l'authentification par carte à puce pour la messagerie | Ce paramètre spécifie si une carte à puce est requise par les terminaux Samsung Knox pour s'authentifier auprès du serveur de messagerie. |
| Autoriser l'utilisateur à modifier les paramètres | Spécifiez si l'utilisateur peut modifier les paramètres de remise.<br>Ce paramètre s'applique uniquement aux terminaux Samsung Knox. |
| **Domaines de messagerie externes** | |
| Liste autorisée des domaines de messagerie externes | Ce paramètre spécifie la liste de domaines vers lesquels un utilisateur peut envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, lorsqu'un utilisateur ajoute un destinataire disposant d'une adresse électronique dans le domaine autorisé à un e-mail ou une entrée de calendrier, aucun message d'avertissement ne s'affiche. Ce paramètre s'applique à l'espace Travail uniquement.<br>Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace. |

| Android : Paramètre de profil de messagerie | Description |
|---|---|
| Liste restreinte des domaines de messagerie externes | Ce paramètre spécifie la liste de domaines vers lesquels les utilisateurs peuvent envoyer des e-mails professionnels et des entrées de calendriers. Par exemple, si un utilisateur tente d'ajouter un destinataire disposant d'une adresse électronique correspondant au domaine limité à un e-mail ou une invitation de calendrier, l'application Messagerie ou Calendrier ne permet pas à l'utilisateur de mener à bien cette opération. Ce paramètre s'applique à l'espace Travail uniquement.<br>Si vous souhaitez indiquer plusieurs noms de domaine, séparez-les par une virgule (,), un point-virgule (;) ou un espace. |

## Windows : paramètres de profil de messagerie

| Windows : paramètre de profil de messagerie | Description |
|---|---|
| **Paramètres de remise** | |
| Type de profil | Ce paramètre spécifie si vous souhaitez que ce profil prenne en charge Exchange ActiveSync ou IBM Notes Traveler.<br>Valeurs possibles :<br>• Exchange ActiveSync<br>• IBM Notes Traveler<br>La valeur par défaut est Exchange ActiveSync. |
| Nom du compte | Ce paramètre spécifie le nom du compte de messagerie professionnel qui apparait sur le terminal Windows. Vous pouvez utiliser une variable telle que %UserEmailAddress%. |
| Intervalle de synchronisation | Ce paramètre spécifie la fréquence à laquelle un terminal Windows télécharge de nouveaux e-mails à partir du serveur de messagerie.<br>Valeurs possibles :<br>• À mesure que les éléments sont reçus<br>• Manuel<br>• 15 minutes<br>• 30 minutes<br>• 60 minutes<br>La valeur par défaut est À mesure que les éléments sont reçus. |

| Windows : paramètre de profil de messagerie | Description |
|---|---|
| Jours de synchronisation | Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal Windows.<br>Valeurs possibles :<br>• Toujours<br>• 3 jours<br>• 7 jours<br>• 14 jours<br>• 1 mois<br>La valeur par défaut est 7 jours. |
| Utiliser SSL | Ce paramètre spécifie si un terminal Windows doit utiliser SSL pour se connecter au serveur de messagerie. |
| **Contenu à synchroniser** | |
| E-mail | Ce paramètre spécifie si un terminal Windows synchronise les e-mails avec le serveur de messagerie. |
| Contacts | Ce paramètre spécifie si un terminal Windows synchronise les contacts avec le serveur de messagerie. |
| Calendrier | Ce paramètre spécifie si un terminal Windows synchronise les entrées de calendrier avec le serveur de messagerie. |
| Tâche | Ce paramètre spécifie si un terminal Windows synchronise les données des tâches avec le serveur de messagerie.<br>Ce paramètre est valide uniquement si le paramètre Type de profil est défini sur Exchange ActiveSync. |

# Protection des données de messagerie électronique envoyées aux terminaux iOS à l'aide de BlackBerry Secure Gateway

BlackBerry Secure Gateway fournit, par le biais de BlackBerry Infrastructure et BlackBerry UEM, une connexion sécurisée au serveur de messagerie de votre entreprise pour les terminaux iOS et iPadOS activés via Contrôles MDM.

Si vous envisagez d'utiliser BlackBerry Secure Gateway, vérifiez que votre organisation dispose des licences adéquates. Pour plus d'informations, reportez-vous au contenu relatif aux licences.

L'activation de BlackBerry Secure Gateway permet aux terminaux d'envoyer et de recevoir des e-mails professionnels sans que vous ayez à exposer votre serveur de messagerie à l'extérieur du pare-feu ou à localiser votre serveur de messagerie dans une zone démilitarisée. Pour activer BlackBerry Secure Gateway, sélectionnez le paramètre Activer BlackBerry Secure Gateway dans le profil de messagerie.

Si votre environnement comprend des terminaux iOS ou iPadOS version 13.0 ou ultérieure et que le serveur de messagerie de votre entreprise est configuré pour utiliser l'authentification moderne Microsoft, vous devez sélectionner le paramètre Utiliser OAuth pour l'authentification dans le profil de messagerie et configurer BlackBerry Secure Gateway afin d'utiliser OAuth pour l'authentification auprès du serveur de messagerie.

Si vous avez configuré des groupes de serveurs pour prendre en charge les connexions régionales à BlackBerry Infrastructure, vous pouvez diriger le trafic de BlackBerry Secure Gateway vers une connexion régionale spécifique en associant le profil de messagerie au groupe de serveurs approprié.

## Configuration des connexions sécurisées à votre serveur de messagerie lorsque vous activez BlackBerry Secure Gateway

Si vous activez BlackBerry Secure Gateway pour obtenir une connexion sécurisée via BlackBerry UEM entre le serveur de messagerie de votre entreprise et des terminaux iOS et iPadOS avec le type d'activation Contrôles MDM, vous devrez peut-être configurer BlackBerry UEM afin d'établir des connexions sécurisées avec Exchange ActiveSync ou le fournisseur d'identité Active Directory.

Si votre environnement inclut des terminaux iOS et iPadOS version 13.0 ou ultérieure qui utilisent l'authentification moderne pour se connecter à Microsoft Exchange Online, vous devez ajouter le certificat (ou le certificat racine) du fournisseur d'identité à BlackBerry UEM. BlackBerry Secure Gateway requiert que le certificat fasse confiance au fournisseur d'identité lorsqu'il établit la connexion. Vous devrez également spécifier le point de terminaison de détection et la ressource du serveur de messagerie pour l'authentification moderne

Si la configuration de votre serveur Exchange ActiveSync exige une connexion TLS, vous devez ajouter le certificat du serveur Exchange ActiveSync (ou le certificat racine) à BlackBerry UEM. BlackBerry Secure Gateway requiert que le certificat fasse confiance au serveur Exchange ActiveSync lorsqu'il établit la connexion TLS/SSL. En fonction des exigences de sécurité de votre serveur Exchange ActiveSync, vous devrez peut-être également mettre à jour la liste de versions TLS et de codages que BlackBerry Secure Gateway peut utiliser pour l'authentification avec Exchange ActiveSync.

# Configurer BlackBerry UEM pour faire confiance au serveur Exchange ActiveSync et le certificat du fournisseur d'identité

**Avant de commencer :**

Exportez les certificats au format X.509 (*.cer, *.der) à partir des serveurs suivants et stockez-les dans un emplacement réseau auquel vous pouvez accéder depuis la console de gestion :

- Serveur Exchange ActiveSync
- Fournisseur d'identité Active Directory si votre environnement inclut iOS ou iPadOS 13,0 et prend en charge l'authentification moderne.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > Certificats approuvés**.
2. Cliquez sur + en regard de **Éléments approuvés du serveur Exchange ActiveSync**.
3. Cliquez sur **Parcourir**.
4. Sélectionnez le fichier de certificat à utiliser.
5. Cliquez sur **Ouvrir**.
6. Saisissez la description du certificat.
7. Cliquez sur **Ajouter**.

# Configurer BlackBerry Secure Gateway afin d'utiliser les versions TLS et les codes pris en charge ou OAuth

Vous pouvez activer BlackBerry Secure Gateway afin qu'il utilise OAuth pour l'authentification moderne. Pour utiliser OAuth, vous avez besoin du point de terminaison du document de découverte du fournisseur d'identité et de l'URL du serveur de messagerie. Pour plus d'informations sur le document de découverte, reportez-vous à la documentation Microsoft.

Vous pouvez également spécifier la version TLS et les codages SSL Microsoft Exchange utilisés par BlackBerry Secure Gateway pour les connexions à Exchange ActiveSync.

1. Sur la barre de menus, cliquez sur **Paramètres > Intégration externe > BlackBerry Secure Gateway**.
2. Pour ajouter ou supprimer une version TLS ou un codage SSL, cliquez sur + dans la table appropriée.
3. Cliquez sur la version TLS ou le codage que vous souhaitez ajouter ou supprimer de la liste **Sélectionné**.
4. Cliquez sur la flèche pour déplacer l'élément dans la liste souhaitée.
5. Cliquez sur **Attribuer**.
6. Pour utiliser l'authentification moderne, sélectionnez **Activer OAuth pour l'authentification du serveur de messagerie**.
7. Dans le champ **Point de terminaison de détection**, saisissez l'URL utilisée par BlackBerry Secure Gateway pour récupérer et mettre en cache le document de découverte du fournisseur d'identité.

   L'URL doit être autre format https://<*fournisseur d'identité*>/.well-known/openid-configuration (par exemple, `https://login.microsoftonline.com/common/.well-known/openid-configuration`). BlackBerry Secure Gateway récupère les documents de découverte v2.0 et sans version et actualise régulièrement les documents mis en cache.
8. Dans le champ **Ressource du serveur de messagerie**, saisissez l'URL du serveur de messagerie spécifié dans le profil de messagerie, en commençant par « https:// » (par exemple. `https://outlook.office365.com`).
9. Cliquez sur **Enregistrer**.

# Activer un BlackBerry Hub unifié sur les terminaux Android Enterprise

BlackBerry Hub est une application Android qui permet aux utilisateurs d'afficher les messages, les notifications et les évènements dans un seul endroit.

Pour autoriser les utilisateurs disposant de terminaux Android Enterprise à afficher les messages professionnels et personnels dans BlackBerry Hub, vous devez vérifier certains paramètres dans BlackBerry UEM.

1. Pour la stratégie informatique qui est attribuée aux utilisateurs, dans la section BlackBerry Productivity Suite, vérifiez que la règle de stratégie informatique Autoriser l'affichage unifié des comptes dans BlackBerry Hub est sélectionnée.
2. Dans la configuration de l'application pour BlackBerry Hub, vérifiez que les éléments suivants sont sélectionnés :
   - Profils IPC
   - Accéder au contenu professionnel

**À la fin :**

Pour plus d'informations sur l'utilisation de BlackBerry Hub sur les terminaux (ajout d'un compte de messagerie ou personnalisation des paramètres BlackBerry Hub, par exemple) reportez-vous au contenu relatif à BlackBerry Hub.

Pour obtenir des informations sur la résolution de problèmes, rendez-vous sur le site http://support.blackberry.com/community pour consulter l'article 37721.

# Extension de la sécurité de la messagerie à l'aide de S/MIME

Vous pouvez renforcer la sécurité de la messagerie des utilisateurs de terminaux iOS et Android en activant S/MIME. S/MIME propose une méthode standard de cryptage et de signature des e-mails. Les utilisateurs peuvent crypter, signer ou crypter et signer les e-mails à l'aide de la protection S/MIME s'ils utilisent un compte de messagerie professionnel prenant en charge les messages protégés par S/MIME sur les terminaux. S/MIME ne peut pas être activé pour les adresses électroniques personnelles.

Les utilisateurs peuvent stocker les certificats S/MIME des destinataires sur leurs terminaux. Les utilisateurs peuvent stocker leurs clés privées sur leurs terminaux ou sur une carte à puce.

Vous pouvez activer S/MIME pour les utilisateurs dans un profil de messagerie. Vous ne pouvez pas contraindre les utilisateurs des terminaux iOS ou Android à utiliser S/MIME. Lorsque l'utilisation de S/MIME est facultative, un utilisateur peut activer S/MIME sur le terminal et choisir de crypter, signer ou crypter et crypter et signer les e-mails.

Les paramètres S/MIME sont prioritaires sur les paramètres PGP. Lorsque la prise en charge S/MIME est définie sur Requise, les paramètres PGP sont ignorés.

## Récupération des certificats S/MIME

Vous pouvez utiliser les profils de récupération de certificat pour autoriser les terminaux Android et iOS à rechercher et récupérer les certificats S/MIME des destinataires à partir des serveurs de certificats LDAP. Si le certificat S/MIME ne figure pas déjà dans un magasin de certificats du terminal, le terminal le récupère et l'importe automatiquement dans le magasin de certificats.

Les terminaux Android et iOS recherchent chaque serveur de certificats LDAP que vous spécifiez dans le profil et récupèrent le certificat S/MIME. S'il existe plusieurs certificats S/MIME et si un terminal n'est pas en mesure de déterminer celui qui a la préférence, le terminal affiche tous les certificats S/MIME pour permettre à l'utilisateur de faire son choix.

Vous pouvez demander à ce que les terminaux utilisent l'authentification simple ou l'authentification Kerberos pour s'authentifier auprès des serveurs de certificats LDAP. Si vous souhaitez que les terminaux utilisent l'authentification simple, vous pouvez inclure les informations d'authentification requises dans des profils de récupération de certificat pour permettre aux terminaux de s'authentifier automatiquement auprès des serveurs de certificats LDAP. Si vous souhaitez que les terminaux utilisent l'authentification Kerberos, vous pouvez inclure les informations d'authentification requises dans des profils de récupération de certificat pour permettre aux terminaux Android et iOS de s'authentifier automatiquement auprès des serveurs de certificats LDAP. Sinon, le terminal demande à l'utilisateur les informations d'authentification requises la première fois que le terminal tente de s'authentifier auprès d'un serveur de certificats LDAP.

Si vous mettez en œuvre l'authentification Kerberos pour l'extraction du certificat S/MIME, vous devez attribuer un profil d'identification unique aux utilisateurs ou groupes d'utilisateurs applicables. Pour plus d'informations sur la création et l'attribution d'un profil d'authentification unique, reportez-vous à la section Configuration de l'authentification avec identification unique pour les terminaux.

Si vous ne créez pas de profil de récupération de certificat et ne l'attribuez pas aux comptes d'utilisateur, groupes d'utilisateurs ou de groupes de terminaux, les utilisateurs doivent manuellement importer les certificats S/MIME à partir d'une pièce jointe à un e-mail professionnel ou d'un ordinateur.

### Créer un profil de récupération de certificat

**Avant de commencer :**

- pour permettre aux terminaux d'approuver les serveurs de certificats LDAP lorsqu'ils établissent des connexions sécurisées, vous devrez peut-être distribuer les certificats d'autorité de certification aux terminaux. Si nécessaire, créez des profils de certificat d'autorité de certification et attribuez-les aux comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Pour plus d'informations sur les certificats d'autorité de certification, reportez-vous à la section Envoi de certificats d'autorité de certification à des terminaux et des applications.
- Si vous mettez en œuvre l'authentification Kerberos pour l'extraction du certificat S/MIME, vous devez attribuer un profil d'identification unique aux utilisateurs ou groupes d'utilisateurs applicables. Pour plus d'informations sur les profils d'identification unique, reportez-vous à la section Configuration de l'authentification avec identification unique pour les terminaux.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > Récupération de certificat**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil de récupération de certificat.
5. Dans le tableau, cliquez sur +.
6. Dans le champ **URL du service**, saisissez le FQDN d'un serveur de certificats LDAP au format ldap://<*fqdn*>:<*port*>. (Par exemple, ldap://serveur01.exemple.com:389).
7. Dans le champ **Base de recherche**, saisissez le DN de base correspondant au point de départ des recherches effectuées sur le serveur de certificats LDAP.
8. Dans la liste déroulante **Étendue de la recherche**, effectuez l'une des opérations suivantes :
   - Pour rechercher l'objet de base uniquement (DN de base), cliquez sur **Base**. Cette option correspond à la valeur par défaut.
   - Pour rechercher un niveau en dessous de l'objet de base, mais pas l'objet de base lui-même, cliquez sur **Un niveau**.
   - Pour rechercher l'objet de base et tous les niveaux situés en dessous, cliquez sur **Sous-arborescence.**
   - Pour rechercher tous les niveaux en dessous de l'objet de base, mais pas l'objet de base lui-même, cliquez sur **Enfants**.
9. Si une authentification est requise, procédez comme suit :
   a) Dans la liste déroulante **Type d'authentification**, cliquez sur **Simple** ou **Kerberos**.
   b) Dans le champ **ID utilisateur LDAP**, saisissez le DN d'un compte doté d'autorisations de recherche sur le serveur de certificats LDAP (par exemple, cn=admin,dc=exemple,dc=com).
   c) Dans le champ **Mot de passe LDAP**, saisissez le mot de passe du compte doté des autorisations de recherche sur le serveur de certificats LDAP.
10. Si nécessaire, cochez la case **Utiliser une connexion sécurisée**.
11. Dans le champ **Délai de connexion**, saisissez le délai, en secondes, durant lequel le terminal attend la réponse du serveur de certificats LDAP.
12. Cliquez sur **Ajouter**.
13. Répétez les étapes 5 à 11 pour chaque serveur de certificats LDAP.
14. Cliquez sur **Ajouter**.

**À la fin :**

- Si nécessaire, classez les profils.

# Identification de l'état des certificats S/MIME sur les terminaux

Vous pouvez utiliser des profils OCSP et CRL pour permettre aux terminaux iOS et Android de vérifier l'état des certificats S/MIME. Vous pouvez attribuer un profil OCSP et un profil CRL à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux.

Les terminaux iOS et Android recherchent chaque répondeur OCSP que vous spécifiez dans un profil OCSP et récupèrent l'état des certificats S/MIME. Les terminaux iOS et Android peuvent envoyer des demandes d'état de certificat à BlackBerry UEM et vous pouvez utiliser des profils CRL pour configurer BlackBerry UEM afin de rechercher l'état des certificats S/MIME via HTTP, HTTPS ou LDAP.

Si vous utilisez Exchange ActiveSync pour obtenir des certificats, les terminaux iOS et Android utilisent Exchange ActiveSync pour vérifier l'état de certificats S/MIME. Si vous utilisez LDAP pour obtenir des certificats, les terminaux iOS et Android utilisent OCSP pour vérifier l'état de certificats. Les terminaux iOS et Android n'utilisent pas de profils OCSP. Les terminaux vérifient le répondeur OCSP du certificat.

Pour plus d'informations sur les indicateurs d'état de certificat, consultez le guide de l'utilisateur du terminal et consultez la section relative aux icônes d'e-mails sécurisés.

## Créer un profil OCSP

Les profils OCSP sont pris en charge sur les terminaux iOS et Android.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > OCSP**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil OCSP.
5. Procédez comme suit :
   a) Dans le tableau, cliquez sur +.
   b) Dans le champ **URL du service**, saisissez l'adresse Web d'un répondeur OCSP.
   c) Dans le champ **Délai de connexion**, saisissez le délai, en secondes, durant lequel le terminal attend la réponse OCSP.
   d) Cliquez sur **Ajouter**.
6. Répétez l'étape 4 pour chaque répondeur OCSP.
7. Cliquez sur **Ajouter**.

**À la fin :** Si nécessaire, classez les profils.

## Créer un profil CRL

Les profils CRL sont pris en charge sur les terminaux iOS et Android.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Certificats > CRL**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil CRL.
5. Pour permettre aux terminaux d'utiliser les URL définies dans le certificat, cochez la case **Utiliser des répondeurs d'extension de certificat**.
6. Effectuez l'une des tâches suivantes :

| Tâche | Étapes |
|---|---|
| Spécifier une configuration HTTP CRL | **a.** Dans la section **HTTP pour CRL**, cliquez sur +.<br>**b.** Saisissez le nom et la description de la configuration HTTP CRL.<br>**c.** Dans le champ **URL du service**, saisissez l'adresse Web d'un répondeur HTTP ou HTTPS.<br>**d.** Cliquez sur **Ajouter**.<br>**e.** Répétez les étapes 1 à 4 pour chaque serveur HTTP ou HTTPS. |
| Spécifier une configuration LDAP CRL | **a.** Dans la section **LDAP pour CRL**, cliquez sur +.<br>**b.** Saisissez le nom et la description de la configuration LDAP CRL.<br>**c.** Dans le champ **URL du service**, saisissez le FQDN d'un serveur LDAP au format ldap://<*fqdn*>:<*port*> (par exemple, ldap://server01.example.com:389). Pour les connexions sécurisées, utilisez le format ldaps://<*fqdn*>:<*port*>.<br>**d.** Dans le champ **Base de recherche**, saisissez le DN de base correspondant au point de départ des recherches effectuées sur le serveur LDAP.<br>**e.** Si nécessaire, cochez la case **Utiliser une connexion sécurisée**.<br>**f.** Dans le champ **ID utilisateur LDAP**, saisissez le DN d'un compte doté d'autorisations de recherche sur le serveur LDAP (par exemple, cn=admin,dc=example,dc=com).<br>**g.** Dans le champ **Mot de passe LDAP**, saisissez le mot de passe du compte doté des autorisations de recherche sur le serveur LDAP.<br>**h.** Cliquez sur **Ajouter**.<br>**i.** Répétez les étapes 1 à 8 pour chaque serveur LDAP. |

**7.** Cliquez sur **Ajouter**.

**À la fin :** Si nécessaire, classez les profils.

# Extension de la sécurité de la messagerie avec PGP

Pour les terminaux iOS et Android, vous pouvez renforcer la sécurité de la messagerie des utilisateurs de terminaux en activant PGP. PGP protège les e-mails des terminaux utilisant le format OpenPGP. Les utilisateurs peuvent signer, crypter ou signer et crypter des e-mails avec la protection PGP lorsqu'ils utilisent une adresse électronique professionnelle. PGP ne peut pas être activé pour les adresses électroniques personnelles.

Vous pouvez activer PGP pour les utilisateurs dans un profil de messagerie. Vous pouvez contraindre les utilisateurs de terminaux iOS et Android à utiliser PGP, interdire l'utilisation de PGP ou la rendre facultative. Lorsque l'utilisation de PGP est facultative (paramètre par défaut), un utilisateur peut activer PGP sur le terminal et choisir de crypter, signer ou crypter et crypter et signer les e-mails.

Pour signer et crypter les e-mails, les utilisateurs doivent stocker des clés PGP pour chaque destinataire sur leurs terminaux. Les utilisateurs peuvent stocker les clés PGP en important des fichiers depuis un e-mail professionnel.

Vous pouvez configurer PGP à l'aide des paramètres de profil de messagerie qui conviennent.

# Application des e-mails sécurisés à l'aide de la classification de messages

La classification de messages permet à votre entreprise de spécifier et d'appliquer des stratégies de sécurité des e-mails et d'ajouter des marques visuelles à des e-mails sur des terminaux iOS et Android. Vous pouvez utiliser BlackBerry UEM pour fournir aux utilisateurs de terminaux iOS et Android des options de classification de messages comparables à celles que vous avez mises à leur disposition pour les applications de messagerie de leur ordinateur. Vous pouvez définir les règles suivantes pour qu'elles s'appliquent aux messages sortants, en fonction des classifications des messages :

- Ajouter une étiquette pour identifier la classification de message (par exemple : confidentiel)
- Ajouter un marqueur visuel à la fin de la ligne d'objet (par exemple : [C])
- Ajouter du texte au début ou à la fin du corps d'un e-mail (par exemple : ce message a été classé comme confidentiel)
- Définir des options S/MIME ou PGP (par exemple : signer et crypter)
- Définir une classification par défaut

Pour les terminaux iOS et Android, vous pouvez utiliser la classification de messages pour exiger que les utilisateurs signent, cryptent ou signent et cryptent les e-mails, ou qu'ils ajoutent des marques visuelles aux e-mails qu'ils envoient de leurs terminaux. Vous pouvez utiliser des profils de messagerie pour les fichiers de configuration de classification de messages (avec extensions de noms de fichiers .json) à envoyer aux terminaux des utilisateurs. Lorsque les utilisateurs répondent à des e-mails avec classification de messages ou rédigent des e-mails sécurisés, la configuration de classification de messages détermine les règles de classification que les terminaux doivent appliquer aux messages sortants.

Les options de protection des messages sur un terminal sont limitées aux types de cryptage et de signature numérique autorisés sur le terminal. Lorsqu'un utilisateur applique une classification de messages à un e-mail sur un terminal, il doit sélectionner l'un des types de protection de message autorisés par cette classification ou accepter le type de protection de message par défaut. Si un utilisateur sélectionne une classification de messages nécessitant la signature, le chiffrement ou la signature et le chiffrement de l'e-mail et si le terminal ne dispose pas d'une configuration S/MIME ou PGP, l'utilisateur ne peut pas envoyer l'e-mail.

Les paramètres S/MIME et PGP sont prioritaires sur la classification de messages. Les utilisateurs peuvent augmenter, mais pas diminuer, les niveaux de classification de messages sur leurs terminaux. Les niveaux de classification de messages sont déterminés par les règles d'e-mails sécurisés de chaque classification.

Lorsque la classification de messages est activée, les utilisateurs ne peuvent pas utiliser BlackBerry Assistant pour envoyer des e-mails à partir de leurs terminaux.

Vous pouvez configurer la classification de messages à l'aide des paramètres de profil de messagerie qui conviennent.

Pour plus d'informations sur la création de fichiers de configuration de classification de messages, rendez-vous sur support.blackberry.com/community pour consulter l'article 36736.

# Créer un profil de messagerie IMAP/POP3

Les profils de messagerie IMAP/POP3 permettent de spécifier la manière dont les terminaux iOS, macOS, Android, et Windows se connectent aux serveurs de messagerie IMAP ou POP3 et synchronisent les e-mails.

Les paramètres de profil requis varient pour chaque type de terminal et dépendent des paramètres que vous sélectionnez.

**Remarque :** BlackBerry UEM envoie le profil de messagerie aux terminaux Android, mais l'utilisateur doit configurer manuellement la connexion au serveur de messagerie.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > E-mail IMAP/POP3**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Dans le champ **Type de messagerie**, sélectionnez le type de protocole de messagerie.
6. Dans le champ **Adresse électronique**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un utilisateur, saisissez l'adresse électronique de l'utilisateur.
   - Si le profil correspond à plusieurs utilisateurs, saisissez `%UserName%`.
7. Dans la section **Paramètres du courrier entrant**, saisissez le nom d'hôte ou l'adresse IP du serveur de messagerie pour la réception du courrier.
8. Si nécessaire, saisissez le port pour la réception du courrier.
9. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.
   - Si le profil correspond à plusieurs utilisateurs, saisissez `%UserName%`.
10. Dans la section **Paramètres du courrier sortant**, saisissez le nom d'hôte ou l'adresse IP du serveur de messagerie pour l'envoi du courrier.
11. Si nécessaire, saisissez le port pour l'envoi du courrier.
12. Si nécessaire, sélectionnez **Authentification requise pour les e-mails sortants** et spécifiez les informations d'identification utilisées pour l'envoi du courrier.
13. Cliquez sur l'onglet correspondant à chaque type de terminal de votre organisation et configurez les valeurs appropriées pour chaque paramètre de profil.
14. Cliquez sur **Ajouter**.

# Paramètres de profil de messagerie IMAP/POP3

Vous pouvez utiliser une variable de paramètre de profil correspondant à un champ de texte pour faire référence à une valeur plutôt que de spécifier la valeur réelle. BlackBerry UEM prend en charge les variables par défaut prédéfinies et les variables personnalisées que vous définissez. Les profils de messagerie IMAP/POP3 sont pris en charge sur les types de terminaux suivants :

- iOS
- macOS
- Android
- Windows

Dans certains cas, la version minimale du système d'exploitation du terminal requis pour prendre en charge un paramètre correspond à une version non prise en charge par BlackBerry UEM. Pour en savoir plus sur les versions prises en charge, consultez la Matrice de compatibilité.

# iOS et macOS : Paramètres de profil de messagerie IMAP/POP3

Ces paramètres s'appliquent également aux terminaux iPadOS.

macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils IMAP/POP3 sont appliqués aux comptes d'utilisateur.

| iOS : paramètre Profil de messagerie IMAP/POP3 | Description |
|---|---|
| Préfixe du chemin IMAP | Ce paramètre spécifie le préfixe de chemin IMAP, si nécessaire.<br>Si nécessaire, contactez votre FAI pour plus d'informations.<br>Ce paramètre est valide uniquement si la valeur du paramètre Type de messagerie est définie sur IMAP. |
| Autoriser le déplacement de messages | Ce paramètre spécifie si les utilisateurs peuvent déplacer les e-mails de ce compte vers un autre compte de messagerie sur un terminal iOS. |
| Autoriser la synchronisation des adresses récentes | Ce paramètre spécifie si un utilisateur de terminal iOS peut synchroniser les adresses récemment utilisées sur les terminaux. |
| Utiliser uniquement dans la messagerie | Ce paramètre spécifie si les applications autres que l'application de messagerie d'un terminal iOS peuvent utiliser ce compte pour envoyer des e-mails. |
| Activer S/MIME | Ce paramètre spécifie si un utilisateur de terminal iOS peut envoyer des e-mails protégés par S/MIME.<br>S/MIME est pris en charge uniquement sur les terminaux qui sont activés avec les commandes MDM. |
| Informations d'identification de signature | Ce paramètre spécifie les identifiants que le terminal utilisera pour signer les e-mails.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.<br>Valeurs possibles :<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>La valeur par défaut est Certificat partagé. |
| Certificat partagé de signature | Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de signer des e-mails.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Certificat partagé. |

| iOS : paramètre Profil de messagerie IMAP/POP3 | Description |
|---|---|
| SCEP de signature | Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis pour signer les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur SCEP. |
| Informations d'identification de connexion de l'utilisateur | Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour obtenir les certificats client requis pour signer les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de connexion est défini sur Identifiants de connexion d'utilisateur. |
| Informations d'identification de cryptage | Ce paramètre spécifie la manière dont les terminaux trouvent les certificats requis pour crypter les messages.<br>Ce paramètre est valide uniquement si le paramètre Activer S/MIME est sélectionné.<br>Valeurs possibles :<br>• Certificat partagé<br>• SCEP<br>• Informations d'identification de l'utilisateur<br>Après avoir sélectionné le type de profil, sélectionnez le profil de certificat partagé, profil SCEP ou profil des informations d'identification de l'utilisateur que vous souhaitez utiliser. |
| Certificat partagé de cryptage | Ce paramètre spécifie le profil de certificat partagé pour un certificat client utilisé par un terminal afin de crypter des e-mails.<br>Les terminaux choisissent le certificat adapté au destinataire pour crypter les messages à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur Certificat partagé. |
| SCEP de cryptage | Ce paramètre spécifie le profil SCEP utilisé par les terminaux pour récupérer les certificats requis et crypter les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur SCEP. |
| Informations d'identification de l'utilisateur de cryptage | Ce paramètre spécifie le profil des informations d'identification de l'utilisateur utilisé par les terminaux pour récupérer les certificats client requis et crypter les e-mails à l'aide de S/MIME.<br>Ce paramètre est valide uniquement si le paramètre Identifiants de cryptage est défini sur Identifiants de connexion d'utilisateur. |

| iOS : paramètre Profil de messagerie IMAP/POP3 | Description |
|---|---|
| Crypter les messages | Ce paramètre spécifie si tous les e-mails doivent être cryptés lorsque l'utilisateur les envoie (Obligatoire) ou si l'utilisateur peut choisir les messages à crypter au moment où il les envoie (Autoriser).<br>Ce paramètre s'applique uniquement si le paramètre Activer S/MIME est sélectionné.<br>Valeurs possibles :<br>• Requise<br>• Autoriser<br>La valeur par défaut est Requis. |
| Autoriser Mail Drop | Ce paramètre spécifie si les utilisateurs peuvent envoyer des fichiers à partir de ce compte avec Mail Drop. |
| VPN par compte | Ce paramètre spécifie le profil VPN utilisé pour la communication réseau de ce compte. Ce paramètre s'applique uniquement aux terminaux exécutant iOS 14 ou version ultérieure ou iPadOS 14 ou version ultérieure. |

# Android : paramètres de profil de messagerie IMAP/POP3

| Android : paramètre de profil de messagerie IMAP/POP3 | Description |
|---|---|
| Préfixe du chemin IMAP | Ce paramètre spécifie le préfixe de chemin IMAP, si nécessaire.<br>Si nécessaire, contactez votre FAI pour plus d'informations.<br>Ce paramètre est valide uniquement si la valeur du paramètre Type de messagerie est définie sur IMAP. |
| Supprimer un e-mail du serveur | Ce paramètre spécifie le moment où supprimer un e-mail du serveur de messagerie.<br>Valeurs possibles :<br>• Jamais<br>• En cas de suppression depuis la boite de réception<br>La valeur par défaut est Jamais.<br>Ce paramètre est valide uniquement si la valeur du paramètre Type de messagerie est définie sur POP3. |

# Windows : paramètres de profil de messagerie IMAP/POP3

| Windows : paramètre de profil de messagerie IMAP/POP3 | Description |
|---|---|
| Supprimer un e-mail du serveur | Ce paramètre spécifie comment les e-mails sont traités lorsqu'un utilisateur les supprime. Les e-mails peuvent être supprimés du serveur (suppression physique) ou supprimés de la boîte de réception mais conservés dans le dossier Corbeille (suppression avec récupération possible).<br>Valeurs possibles :<br>• Supprimer définitivement<br>• Supprimer (récupération possible)<br>La valeur par défaut est Supprimer (récupération possible).<br>Ce paramètre est valide uniquement si le paramètre Type de messagerie est défini sur IMAP. |
| Domaine | Ce paramètre spécifie le nom de domaine du serveur de messagerie. |
| Intervalle de synchronisation | Ce paramètre spécifie la fréquence à laquelle un terminal Windows télécharge du nouveau contenu à partir du serveur de messagerie.<br>Valeurs possibles :<br>• Manuel<br>• 15 minutes<br>• 30 minutes<br>• 60 minutes<br>• 2 heures<br>La valeur par défaut est 15 minutes. |
| Montant de récupération initial | Ce paramètre spécifie le nombre de jours passés afin de synchroniser les e-mails et données de l'organiseur avec un terminal Windows.<br>Valeurs possibles :<br>• Tout<br>• 7 jours<br>• 14 jours<br>• 30 jours<br>La valeur par défaut est 7 jours. |
| Utiliser uniquement le réseau cellulaire et non Wi-Fi | Ce paramètre indique si des e-mails sont envoyés et reçus uniquement sur le réseau mobile. |

# Configuration des profils CardDAV et CalDAV pour les terminaux iOS et macOS

Vous pouvez utiliser les profils CardDAV et CalDAV pour permettre aux terminaux iOS, iPadOS et macOS d'accéder aux informations de contact et de calendrier sur un serveur distant. Vous pouvez attribuer des profils CardDAV et CalDAV à des comptes d'utilisateur, groupes d'utilisateurs ou groupes de terminaux. Plusieurs terminaux peuvent accéder à la même information.

macOS applique les profils aux terminaux ou comptes d'utilisateur. Les profils CardDAV et CalDAV sont appliqués aux comptes d'utilisateur.

## Créer un profil CardDAV

**Avant de commencer :**

- Vérifiez que le terminal peut accéder à un serveur CardDAV actif.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > CardDAV**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Tapez l'adresse du serveur pour le profil. C'est le FQDN de l'ordinateur qui héberge l'application Calendrier.
6. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.
   - Si le profil correspond à plusieurs utilisateurs, saisissez `%UserName%`.
7. Si nécessaire, entrez le port utilisé pour le serveur CardDAV.
8. Si nécessaire, sélectionnez la case **Utiliser SSL** et entrez l'URL du serveur SSL.
9. Si nécessaire, dans le champ **VPN par compte**, sélectionnez le profil VPN que vous souhaitez utiliser pour la communication réseau de ce compte.
10. Cliquez sur **Ajouter**.

**À la fin :** attribuez le profil aux utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux.

## Créer un profil CalDAV

**Avant de commencer :**

- Vérifiez que le terminal peut accéder à un serveur CalDAV actif.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **E-mail, calendrier et contacts > CalDAV**.
3. Cliquez sur +.
4. Saisissez le nom et la description du profil.
5. Tapez l'adresse du serveur pour le profil. C'est le FQDN de l'ordinateur qui héberge l'application Calendrier.
6. Dans le champ **Nom d'utilisateur**, effectuez l'une des opérations suivantes :
   - Si le profil concerne un seul utilisateur, indiquez le nom d'utilisateur.

- Si le profil correspond à plusieurs utilisateurs, saisissez `%UserName%`.

7. Si nécessaire, entrez le port utilisé pour le serveur CalDAV.
8. Si nécessaire, sélectionnez la case **Utiliser SSL** et entrez l'URL du serveur SSL.
9. Si nécessaire, dans le champ **VPN par compte**, sélectionnez le profil VPN que vous souhaitez utiliser pour la communication réseau de ce compte.
10. Cliquez sur **Ajouter**.

**À la fin :** attribuez le profil aux utilisateurs, aux groupes d'utilisateurs ou aux groupes de terminaux.

# Informations juridiques



Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTUELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada