



BlackBerry AtHoc

Authentication Smart Card

7.17

Contents

- Qu'est-ce que l'authentification par carte à puce ?..... 4**
 - Fonctionnement de l'authentification par carte à puce dans BlackBerry AtHoc..... 4
- Activer l'authentification par carte à puce pour les opérateurs..... 5**
 - Configuration du système de gestion BlackBerry AtHoc..... 5
 - Configuration IIS..... 5
- Activer l'authentification par carte à puce pour l'application mobile.....6**
- Activer l'authentification par carte à puce pour l'application de bureau..... 7**
 - Configuration du système de gestion BlackBerry AtHoc..... 7
 - Configuration IIS..... 7
- Activer l'authentification par carte à puce pour Self Service..... 8**
- Mettre à jour le serveur d'applications..... 9**
- Mettre à jour le serveur de base de données..... 10**
- Déterminer l'expression régulière..... 12**
 - Outil de test des expressions régulières..... 12
 - Mettre à jour la base de données..... 13
- Dépannage de l'authentification par carte à puce..... 14**
- Annexe A : Récupérer les informations relatives aux certificats..... 15**
- Portail de support client BlackBerry AtHoc..... 16**
- Commentaires sur la documentation.....17**
- Informations juridiques..... 18**

Qu'est-ce que l'authentification par carte à puce ?

Lorsque l'authentification par carte à puce est activée, en plus de l'authentification standard par nom d'utilisateur/mot de passe, les utilisateurs peuvent se connecter à BlackBerry® AtHoc® en insérant leur carte à puce dans un lecteur de carte ou en sélectionnant un certificat valide sur l'application mobile.

Si vous choisissez d'exiger des opérateurs qu'ils se connectent à l'aide de cartes à puce, les modifications suivantes interviennent du côté administratif du système BlackBerry AtHoc :

- Dans une entreprise, toutes les sous-organisations héritent de la méthode d'authentification par carte à puce uniquement.
- Dans une super entreprise, toutes les sous-entreprises et leurs sous-organisations héritent de la méthode d'authentification par carte à puce uniquement.
- L'écran de connexion continue d'afficher les champs **Nom d'utilisateur** et **Mot de passe**, car jusqu'à ce qu'un utilisateur tente de se connecter, le système ne sait pas à quelle organisation appartient l'utilisateur et quelles restrictions, le cas échéant, l'organisation de l'utilisateur a imposées à l'authentification.
- Lorsque l'utilisateur tente de se connecter avec un nom d'utilisateur ou un mot de passe, le système renvoie un message d'erreur l'informant qu'il doit utiliser sa carte à puce pour l'authentification du système.

Fonctionnement de l'authentification par carte à puce dans BlackBerry AtHoc

Lorsque l'authentification par carte à puce est activée, l'attribut MID (ID de mappage) de l'opérateur est utilisé pour authentifier l'opérateur lors de la connexion. Les données de l'ID de mappage proviennent d'une des sources suivantes :

- Synchronisation avec l'attribut Active Directory (sAMAccountName, userprincipalname ou mail) lors de l'utilisation de l'outil Client de synchronisation des utilisateurs.
- Importation d'utilisateur à l'aide de l'option Importer du gestionnaire des utilisateurs finaux dans BlackBerry AtHoc incluant la colonne ID de mappage.
- Mise à jour manuelle de l'ID de mappage d'un opérateur dans le gestionnaire des utilisateurs finaux dans BlackBerry AtHoc.

BlackBerry AtHoc utilise une expression régulière pour extraire la valeur de l'ID de mappage de l'un des champs d'entête HTTP contenant les données de certificat. BlackBerry AtHoc compare ensuite cet ID de mappage avec l'ID de mappage de l'opérateur pour déterminer son identité. Les valeurs du champ d'entête HTTP et de l'expression régulière sont spécifiées dans la base de données et peuvent être modifiées. Cependant, ces valeurs s'appliquent à l'ensemble du système et ne peuvent pas être différentes pour chaque organisation.

Le code de niveau intermédiaire tente d'utiliser la variable HTTP_CAC_VARIABLE principale, le cas échéant, et valide l'opérateur. Si aucun opérateur valide n'est trouvé, le code de niveau intermédiaire tente d'utiliser la variable ALT_HTTP_CAC_VARIABLE pour valider l'opérateur.

Si aucun opérateur valide n'est trouvé, le code de niveau intermédiaire tente d'utiliser le nom alternatif du sujet pour valider l'opérateur.

Le fichier de code source de connexion est `wwwroot\client\dotnet\Controllers\SmartCardController.cs`.

Activer l'authentification par carte à puce pour les opérateurs

Lorsque l'authentification par carte à puce est activée, en plus de l'authentification standard par nom d'utilisateur/mot de passe, les utilisateurs peuvent se connecter à BlackBerry AtHoc en insérant leur carte à puce dans un lecteur de carte, puis en saisissant un code PIN. Sur l'application mobile, ils peuvent sélectionner un certificat valide. Lorsque l'authentification par carte à puce est requise, les utilisateurs doivent accéder à BlackBerry AtHoc en insérant leur carte à puce dans un lecteur de carte, puis en saisissant un code PIN.

Note: Pour utiliser cette option, vous devez configurer des ID de mappage pour chaque utilisateur via le gestionnaire des utilisateurs du système de gestion BlackBerry AtHoc.

Configuration du système de gestion BlackBerry AtHoc

Utilisez le système de gestion BlackBerry AtHoc afin d'activer la connexion par carte à puce pour les opérateurs.

1. Connectez-vous à la console de gestion BlackBerry AtHoc en tant qu'administrateur.
2. Passez à l'organisation **Configuration du système (3)**.
3. Dans la barre de navigation, cliquez sur .
4. Dans la section **Configuration du système**, cliquez sur **Politique de sécurité**.
5. Dans la section **Authentification par carte à puce**, sélectionnez **Activée** en regard de **Connexion par carte à puce**.
6. Vous pouvez également exiger l'authentification par carte à puce en sélectionnant **Exiger l'authentification par carte à puce**.
7. Cliquez sur **Enregistrer**.

Note: Il s'agit d'un paramètre à l'échelle du système qui s'applique à toutes les organisations.

Configuration IIS

L'authentification par carte à puce pour la connexion de l'opérateur nécessite les paramètres suivants dans IIS. Dans la fonctionnalité Paramètres SSL de l'application Web cliente, cochez la case **Exiger SSL** et sélectionnez l'option **Exiger** sous Certificats client.

Table 1: Paramètres SSL par version BlackBerry AtHoc

Version	Notes
Tout	Site Web par défaut > Paramètres SSL Obligatoire + Ignorer
Version 7.15 ou ultérieure	Site Web par défaut > Client > SmartCard > Paramètres SSL : Obligatoire + Accepter Site Web par défaut > SelfService > AuthCAC > Paramètres SSL : Obligatoire + Accepter

Activer l'authentification par carte à puce pour l'application mobile

Lorsque l'authentification par carte à puce est activée pour l'application mobile, lorsqu'un opérateur démarre la publication d'alertes, le résumé de rapport ou les flux de réponse du responsable de la responsabilité pour le compte d'autres personnes (ROBO), une fenêtre s'affiche pour permettre à l'opérateur de sélectionner un certificat valide. Le certificat doit déjà être présent sur le terminal de l'opérateur. Lorsqu'un certificat valide est sélectionné, l'opérateur peut alors terminer le flux. Si le certificat sélectionné n'est pas valide, l'opérateur est redirigé vers l'écran de connexion nom d'utilisateur et mot de passe. Lorsque l'opérateur sélectionne un certificat valide, il est redirigé vers l'application mobile pour terminer le flux. Si le certificat sélectionné n'est pas valide ou si l'authentification par smart card échoue, l'opérateur est redirigé vers l'authentification à l'aide de son nom d'utilisateur et de son mot de passe.

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur.
2. Cliquez sur .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Sur l'écran **Authentification de l'utilisateur**, dans la section **Méthodes d'authentification activées**, sélectionnez **Activer** en regard de **Carte à puce**.
5. Dans la section **Attribuer des méthodes d'authentification aux applications**, dans la section **Application mobile**, sélectionnez **Carte à puce**.

Note: Cette section s'affiche uniquement lorsque la passerelle de l'application mobile est activée et configurée.

6. Cliquez sur **Enregistrer**.

Note: La méthode d'authentification Nom d'utilisateur et mot de passe est activée par défaut et ne peut pas être désélectionnée. Si l'authentification par carte à puce est activée, il s'agit de la méthode d'authentification principale.

Activer l'authentification par carte à puce pour l'application de bureau

Cette section contient des informations sur les mises à jour de configuration liées au système de gestion BlackBerry AtHoc et à IIS nécessaires pour activer l'authentification par carte à puce pour l'application de bureau BlackBerry AtHoc.

Configuration du système de gestion BlackBerry AtHoc

Vous pouvez activer l'authentification par carte à puce pour l'application de bureau dans le système de gestion BlackBerry AtHoc.

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur.
2. Cliquez sur .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Dans la fenêtre **Authentification de l'utilisateur**, dans la section **Méthodes d'authentification activées**, sélectionnez **Activer** en regard de **Carte à puce**.
5. Dans la section **Attribuer des méthodes d'authentification aux applications**, accédez à la section **Application de bureau** et sélectionnez **Carte à puce** dans la liste **Méthode d'authentification**.
6. Sélectionnez le nombre de certificats client à collecter dans la liste. La valeur recommandée est 3.
7. Si vous le souhaitez, dans le champ **Expression régulière**, saisissez une expression régulière au format suivant : `UID=(? <edipi>\d{8,10})`. Contactez l'assistance client BlackBerry AtHoc pour configurer ce champ.
8. Si vous le souhaitez, dans le champ **Expression régulière client**, saisissez une expression régulière au format suivant : `. *?( ^ ) ( ? : ( ? ! \ s - [ A | | E | | S ] ) . ) *`. Ce format extrait les informations du nom d'objet du certificat client pour trouver les certificats identiques pour l'authentification. L'expression régulière fournie dans l'interface utilisateur est un exemple d'expression qui peut ne pas convenir à votre environnement. Vous pouvez créer votre propre expression régulière ou contacter l'assistance client BlackBerry AtHoc pour configurer ce champ.
9. Vous pouvez également sélectionner **Créer un nouvel utilisateur si aucun compte n'est trouvé** afin de configurer l'application de bureau pour créer un utilisateur au moment de la connexion, si l'utilisateur n'existe pas encore.
10. Cliquez sur **Enregistrer**.

Note: Ce paramètre doit être configuré pour chaque organisation.

Configuration IIS

L'authentification par carte à puce pour l'application de bureau requiert les paramètres suivants dans IIS.

Dans la fonctionnalité **Paramètres SSL**, sous l'application Web cliente, cochez la case **Exiger SSL**.

L'authentification par carte à puce pour l'application de bureau fonctionne avec toutes les options disponibles sous Certificats client. Toutefois, pour éviter que les utilisateurs finaux ne soient invités à saisir leur code PIN à intervalles de quelques minutes, sélectionnez l'option **Ignorer**.

Activer l'authentification par carte à puce pour Self Service

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur.
2. Cliquez sur .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Sur l'écran **Authentification de l'utilisateur**, dans la section **Méthodes d'authentification activées**, sélectionnez **Activer** en regard de **Carte à puce**.
5. Dans la section **Attribuer des méthodes d'authentification aux applications**, accédez à la section **Self Service** et sélectionnez **Carte à puce** dans la liste **Méthode d'authentification**.
6. Cliquez sur **Enregistrer**.

Mettre à jour le serveur d'applications

Le serveur d'applications BlackBerry AtHoc est pris en charge sous Windows 2016 et versions ultérieures.

Pour activer l'authentification par carte à puce, vous devez ajouter la nouvelle clé suivante dans le registre :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL Value
name: ClientAuthTrustMode Value type: REG_DWORD Value data: 2.

Mettre à jour le serveur de base de données

Les valeurs du serveur de base de données qui sont utilisées pour l'authentification par carte à puce sont stockées dans l'onglet GLB_CONFIG_TAB de la base de données ngaddata. Ces valeurs comprennent les éléments suivants :

- Nom de l'entête HTTP contenant les informations.
- Expression régulière utilisée pour extraire les informations.

L'option Exiger une carte à puce apparaît lorsque vous sélectionnez Connexion par carte à puce.

La valeur SMART_CARD_ENFORCED est présente dans l'onglet PRV_SECURITY_POLICY_TAB.

Les paramètres de carte à puce suivants sont présents dans l'onglet GLB_CONFIG_TAB :

- ALT_HTTP_CAC_REGEX
- ALT_HTTP_CAC_VARIABLE
- CAC_CHECK_PRESENT
- CAC_CHECK_VALID
- CAC_REGEX
- CAC_SAN_REGEX
- HTTP_CAC_REGEX
- HTTP_CAC_VARIABLE

Table 2: Définition des paramètres de la carte à puce

KEY_NAME	Notes
ALT_HTTP_CAC_REGEX	(Connexion opérateur) Expression régulière alternative utilisée pour extraire l'ID de mappage du certificat CAC.
ALT_HTTP_CAC_VARIABLE	(Connexion opérateur) Variable d'entête HTTP alternative qui contient l'ID de mappage du certificat CAC.
CAC_CHECK_PRESENT	(Connexion opérateur) Indique si le système doit vérifier la présence du certificat CAC.
CAC_CHECK_VALID	(Connexion opérateur) Indique si le système doit vérifier la validité du certificat CAC.
CAC_REGEX	Expression régulière principale utilisée pour extraire l'ID de mappage des données de certificat transmises par l'application de bureau BlackBerry AtHoc lors de l'ouverture de session.
CAC_SAN_REGEX	(Connexion opérateur) Expression régulière alternative utilisée pour extraire l'adresse e-mail du nom alternatif de l'objet dans le certificat.
HTTP_CAC_REGEX	Expression régulière principale utilisée pour extraire l'ID de mappage du certificat lors de la connexion de l'opérateur.
HTTP_CAC_VARIABLE	Variable d'entête HTTP principale utilisée pour rechercher l'ID de mappage lors de la connexion de l'opérateur.

Table 3: Corrélation des paramètres de la carte à puce entre la base de données et l'interface utilisateur

KEY_NAME	Visible dans le système de gestion
ALT_HTTP_CAC_REGEX	Non
ALT_HTTP_CAC_VARIABLE	Non
CAC_CHECK_PRESENT	Non
CAC_CHECK_VALID	Non
CAC_REGEX	Non
CAC_SAN_REGEX	Non
HTTP_CAC_REGEX	Non
HTTP_CAC_VARIABLE	Non

Déterminer l'expression régulière

Les trois expressions régulières (regex) suivantes permettent d'extraire l'ID de mappage de l'utilisateur :

1. HTTP_CAC_REGEX : Regex principale de BlackBerry AtHoc pour la connexion de l'opérateur.
2. ALT_HTTP_CAC_REGEX : Première regex alternative de BlackBerry AtHoc pour la connexion de l'opérateur.
3. CAC_SAN_REGEX : Deuxième regex alternative de BlackBerry AtHoc pour la connexion de l'opérateur.

Le serveur BlackBerry AtHoc essaie d'abord HTTP_CAC_REGEX. Si ALT_HTTP_CAC_REGEX renvoie une chaîne vide, le serveur essaie CAC_SAN_REGEX. Si aucune de ces expressions régulières ne permet d'extraire une valeur ou si les informations récupérées sont incorrectes, la connexion par carte à puce échoue.

Pour identifier le problème, vérifiez le certificat et assurez-vous qu'au moins une des expressions régulières extrait la valeur. Pour plus d'informations, reportez-vous à [Annexe A : Récupérer les informations relatives aux certificats](#).

Outil de test des expressions régulières

Vous pouvez utiliser un outil de test des expressions régulières en ligne pour tester les expressions régulières. Saisissez les données et ajustez l'expression régulière jusqu'à ce que l'ID de mappage soit extrait des données.

Le code SQL permettant de récupérer l'expression régulière actuelle de la base de données est le suivant :

```
SELECT value FROM GLB_CONFIG_TAB where KEY_NAME = 'ALT_HTTP_CAC_REGEX'
```

Si les valeurs des expressions régulières préconfigurées ne permettent pas d'extraire les informations correctes, modifiez l'expression régulière stockée dans ALT_HTTP_CAC_REGEX. La valeur par défaut est la suivante :

```
(?<MID>\d{8,10})(?!.*\d)
```

Où :

- ?<MID> correspond au groupe nommé MID requis par le code de niveau intermédiaire. Le regex restant entre parenthèses avec ?<MID> correspond à la sous-expression : \d{8,10}.
- \d correspond à n'importe quel chiffre décimal et \d{8,10} à n'importe quel nombre compris entre 8 et 10 chiffres.
- (?!.*\d) correspond à un point 0 fois ou plus, à un chiffre décimal une fois, et cette expression est utilisée par (?<MID>\d{8,10}) pour extraire des nombres de 8 à 10 chiffres. Par exemple :
 - 0069651550.CBP est évalué à 0069651550 (Correct : extrait entre 8 et 10 chiffres à gauche de la décimale.)
 - FIRST.LAST.MI.1233837489 est évalué à 1233837489 (Correct : extrait entre 8 et 10 chiffres à droite de la dernière décimale.)
 - 1234567890.CBP.11223344 est évalué à 11223344 (Correct : extrait entre 8 et 10 chiffres du dernier nombre.)
 - 1234567890.CBP.112233445566 est évalué à 2233445566 (Incorrect : tronque les chiffres lorsqu'il y en a plus de 10.) Vous devez mettre à jour le regex : (?<MID>\d{8,12}) fonctionnera.)

Pour plus d'informations sur la syntaxe des expressions régulières .Net, reportez-vous à :

<https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference>

Si des modifications sont nécessaires pour s'adapter à un format différent, deux options s'offrent à vous :

1. Envoyez les données ci-dessus au service client BlackBerry AtHoc en demandant aux ingénieurs de déterminer la nouvelle expression régulière.

2. Déterminez vous-même l'expression régulière.

Mettre à jour la base de données

Une fois que vous avez trouvé une bonne expression régulière, mettez-la à jour dans la base de données. Utilisez le SQL suivant pour mettre à jour la base de données avec la nouvelle expression régulière. Remplacez 'new_expression' par la nouvelle expression régulière :

```
UPDATE GLB_CONFIG_TAB SET VALUE = 'new_expression' WHERE KEY_NAME =  
'ALT_HTTP_CAC_REGEX'
```

Dépannage de l'authentification par carte à puce

Si l'authentification par carte à puce échoue après avoir été configurée, cela peut être dû au format de la chaîne CN du certificat. BlackBerry AtHoc dispose de trois expressions régulières permettant de valider l'ID de mappage :

- HTTP_CAC_REGEX
- ALT_HTTP_CAC_REGEX
- CAC_SAN_REGEX

Ces expressions régulières se trouvent dans `ngaddata.glb_config_tab`. BlackBerry AtHoc tente d'analyser le MID à l'aide de HTTP_CAC_REGEX. Si cela échoue, il tente d'analyser le MID à l'aide de ALT_HTTP_CAC_REGEX. Si cela échoue également, il tente d'analyser le MID à l'aide de CAC_SAN_REGEX.

Parfois, le certificat peut être supprimé de l'entête par un serveur proxy, ce qui entraîne l'échec de la validation. Dans d'autres cas, l'expression régulière n'a pas pu analyser les données. Dans un premier temps, vérifiez que les détails du certificat sont bien transmis à BlackBerry AtHoc. Utilisez la page de test décrite dans [Annexe A : Récupérer les informations relatives aux certificats](#).

Reportez-vous à l'exemple d'entrée de journal détaillée ci-dessous et notez que l'objet est manquant.

Si vous obtenez une erreur 403 qui empêche l'affichage de la page de connexion, désélectionnez Exiger SSL dans IIS. Sinon, l'appel à GetCACMID n'est pas effectué.

Si les informations du certificat n'apparaissent pas, cela peut être dû aux paramètres SSL dans IIS, ou à un proxy qui supprime les informations de la demande.

Il est possible que les informations du certificat soient disponibles, mais pas le certificat. La propriété CAC_CHECK_PRESENT peut être définie sur N pour contourner ce problème. Ce paramètre n'est pas exposé dans l'interface utilisateur.

Exemple d'entrée de journal détaillée :

```
<event>
<eventId>12445</eventId>
<type>VERBOSE</type>
<time>02/03/2015 15:36:53.350</time>
<server>D1ASEPRIC090</server>
<categorySource>Management System</categorySource>
<assembly>MSDotNetClient.dll</assembly>
<module>AuthController</module>
<member>GetCACMID</member>
<shortMessage> CAC: Issuer: SerialNumber: Subject: Valid From: 2/3/2015 3:36:53 PM
Valid Until: 2/3/2015 3:36:53 PM IsValid: True CertEncoding: 0 Cookie: Present:
False </shortMessage>
. . . .
```

Annexe A : Récupérer les informations relatives aux certificats

Vous pouvez récupérer les informations relatives aux certificats à l'aide des deux méthodes suivantes :

- Utiliser la page de test du système de gestion
- Utiliser un exemple de certificat

Utiliser la page de test du système de gestion

La page de test se trouve à l'adresse suivante : <https://<server>/client/smartcard/info>

Si cette URL de test ne fonctionne pas, activez la journalisation détaillée et recherchez les détails du certificat dans le journal des événements BlackBerry AtHoc. Recherchez le module AuthController ou le membre GetCACMID. Désactivez la journalisation détaillée après avoir trouvé les détails du certificat.

Utiliser un exemple de certificat

Demandez au client de fournir un exemple de certificat pour déterminer si l'expression régulière peut analyser le MID. Vous devrez peut-être demander plusieurs exemples à des fins de comparaison.

Pour ouvrir le certificat d'un client, procédez comme suit :

1. Dans le **menu Démarrer**, saisissez **MMC** dans la zone de recherche et appuyez sur **Entrée**.
2. Une fois le MMC ouvert, cliquez sur **FICHIER** et sélectionnez **Ajouter/Supprimer le composant logiciel enfichable**.
3. Sélectionnez le composant logiciel enfichable Certificats situé à gauche, puis cliquez sur **Ajouter**.
4. Lorsque vous y êtes invité, sélectionnez **Mon compte d'utilisateur**.
5. Cliquez sur **Terminer**.
6. Cliquez sur **OK** pour fermer le menu et revenir à la page principale de la console.
7. Recherchez le certificat de l'utilisateur et ouvrez-le.
8. Dans la fenêtre **Certificat**, cliquez sur l'onglet **Détails**.
9. Assurez-vous que l'option **Afficher** : est définie sur **<All>**.
10. Faites défiler vers le bas et sélectionnez **Objet**. Le MID s'affiche dans le champ ci-dessous. Il s'affiche à côté de la valeur CN.
11. Copiez les détails ou cliquez sur **Copier dans un fichier....** Les informations contenues dans CN sont utilisées pour déterminer l'expression régulière à utiliser, qui remplacera la valeur existante dans glb_config_tab.

Certains clients dotés de systèmes OnPrem utilisent plusieurs types de cartes à puce et l'une des expressions régulières. Dans ce cas, il est nécessaire de coordonner avec le client les regex à mettre à jour (CAC_REGEX ou ALT_HTTP_CAC_REGEX) en présence d'une solution pour le CAC/PIV qui pose problème.

Essayez d'obtenir trois ou quatre certificats utilisateur et comparez-les.

Portail de support client BlackBerry AtHoc

Les clients BlackBerry AtHoc peuvent obtenir plus d'informations sur les produits BlackBerry AtHoc ou obtenir des réponses à leurs questions sur leurs systèmes BlackBerry AtHoc sur le portail de support client :

<https://www.blackberry.com/us/en/support/enterpriseapps/athoc>

Le portail de support client BlackBerry AtHoc fournit également une assistance via une formation assistée par ordinateur, des listes de contrôle d'opérateur, des ressources conformes aux bonnes pratiques, des manuels de référence et des guides de l'utilisateur.

Commentaires sur la documentation

L'équipe de documentation de BlackBerry AtHoc s'efforce de fournir une documentation technique précise, utile et à jour. Si vous avez des commentaires ou des retours à faire sur la documentation de BlackBerry AtHoc, envoyez un e-mail à l'adresse athocdocfeedback@blackberry.com. Veuillez inclure le nom et le numéro de version du document dans votre e-mail.

Pour consulter d'autres documents de BlackBerry AtHoc, rendez-vous sur <https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc>. Pour consulter les guides d'action rapide de BlackBerry AtHoc, reportez-vous à la page <https://docs.blackberry.com/en/id-comm-collab/blackberry-athoc/Quick-action-guides/latest>.

Pour plus d'informations sur les produits BlackBerry AtHoc ou si vous avez besoin de réponses à des questions sur votre système BlackBerry AtHoc, rendez-vous sur le portail d'assistance clientèle à l'adresse <https://www.blackberry.com/us/en/support/enterpriseapps/athoc>.

Informations juridiques

©2023 BlackBerry Limited. Les marques commerciales, notamment BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE et SECUSMART sont des marques commerciales ou des marques déposées de BlackBerry Limited, ses filiales et/ou sociétés affiliées, utilisées sous licence, et les droits exclusifs de ces marques commerciales sont expressément réservés. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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, DÉLICTELS 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