BlackBerry 2FA

Guide d'administration

Table des matières

À propos de BlackBerry 2FA

BlackBerry 2FA protège l'accès aux ressources critiques de votre organisation à l'aide de l'authentification à deux facteurs. Le produit utilise un mot de passe que les utilisateurs saisissent et une invite sécurisée sur leur terminal mobile chaque fois qu'ils tentent d'accéder à des ressources. BlackBerry 2FA prend également en charge l'utilisation de jetons de mot de passe à usage unique (OTP) basés sur des normes.

Vous gérez les utilisateurs de BlackBerry 2FA depuis la console de gestion BlackBerry UEM Cloud ou BlackBerry UEM. Vous pouvez également utiliser BlackBerry 2FA sur des terminaux qui ne sont pas gérés par BlackBerry UEM Cloud ou BlackBerry UEM. BlackBerry 2FA prend en charge les terminaux iOS et Android disposant uniquement d'un conteneur BlackBerry Dynamics, les terminaux gérés par des systèmes MDM tiers ou les terminaux non gérés.

Vous pouvez utiliser BlackBerry 2FApour protéger une large gamme de systèmes, parmi lesquels des VPN, des systèmes compatibles RADIUS, des applications personnalisées qui utilisent un API REST et des services cloud conformes à SAML lorsqu'ils sont utilisés de manière conjointe avec BlackBerry Enterprise Identity.

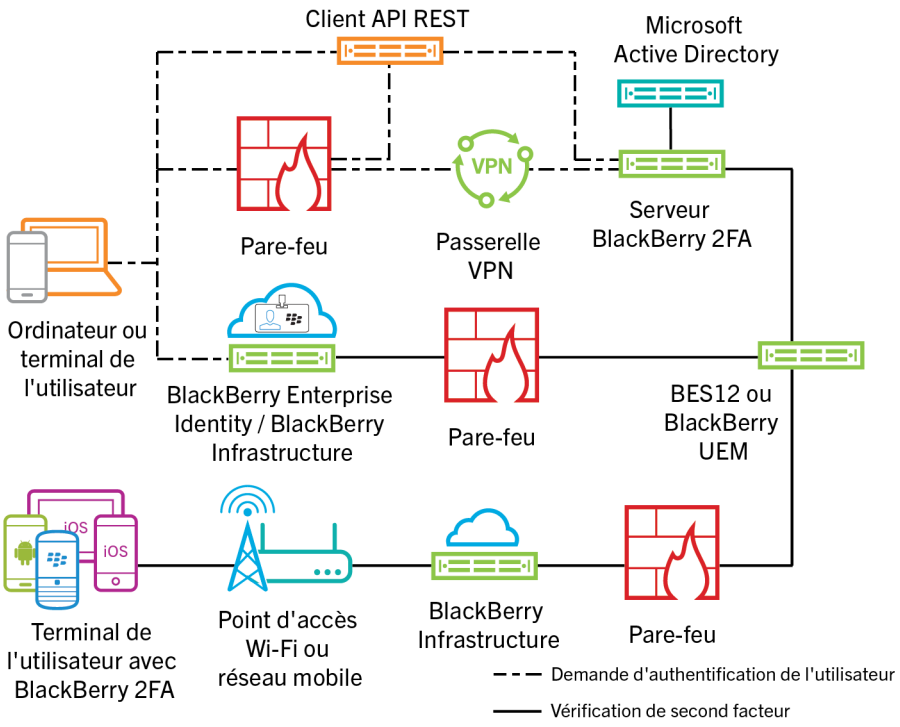
La configuration de BlackBerry 2FA pour une utilisation avec des terminaux mobiles est simple. Le premier facteur d'authentification, le mot de passe, peut être un mot de passe du répertoire ou du conteneur de l'utilisateur. Le second facteur d'authentification, l'invite du terminal, nécessite une application sur le terminal qui déclenche une validation sécurisée du terminal. Pour les terminaux iOS et Android, BlackBerry 2FA est inclus dans BlackBerry UEM Client. Ils sont installés au cours de l'activation ou par les utilisateurs à votre demande. Pour les terminaux BlackBerry 10 gérés, vous devez déployer une application BlackBerry 2FA distincte ou demander aux utilisateurs de l'installer.

La configuration de BlackBerry 2FA pour les utilisateurs sans terminaux mobiles est également simple. Les jetons OTP basés sur des normes sont enregistrés dans la console BlackBerry UEM et attribués aux utilisateurs. Le premier facteur d'authentification est le mot de passe du répertoire de l'utilisateur et le second facteur est le code dynamique qui apparaît sur l'écran du jeton. Pour plus d'informations, reportez-vous au contenu relatif à l'administration de BlackBerry 2FA.

Le serveur BlackBerry 2FA est un composant facultatif déployé en cas d'utilisation du produit de manière conjointe avec des systèmes RADIUS, comme la plupart des VPN, ou qui est utilisé avec des applications qui appellent l'API REST du produit. Le serveur BlackBerry 2FA n'est pas requis pour les déploiements qui utilisent uniquement Enterprise Identity, mais il peut être déployé dans les cas où vous souhaitez utiliser l'authentification à deux facteurs pour les services cloud et les autres systèmes pris en charge. Pour plus d'informations, reportez-vous aux tableaux de compatibilité du serveur BlackBerry 2FA, au contenu relatif à l'installation et à la mise à niveau du serveur BlackBerry 2FA et au contenu relatif à la configuration du serveur BlackBerry 2FA.

Pour utiliser BlackBerry 2FA, vous devez acheter des licences utilisateur pour les éditions Collaboration, Application ou Contenu de BlackBerry Enterprise Mobility Suite, ou des licences utilisateur 2FA séparées. Pour l'édition Collaboration, BlackBerry 2FA peut être utilisé uniquement pour l'authentification auprès des applications BlackBerry et de Microsoft Office 365. Pour plus d'informations sur BlackBerry 2FA, y compris sur le mode d'achat de 2FA, consultez les informations sur blackberry.com.

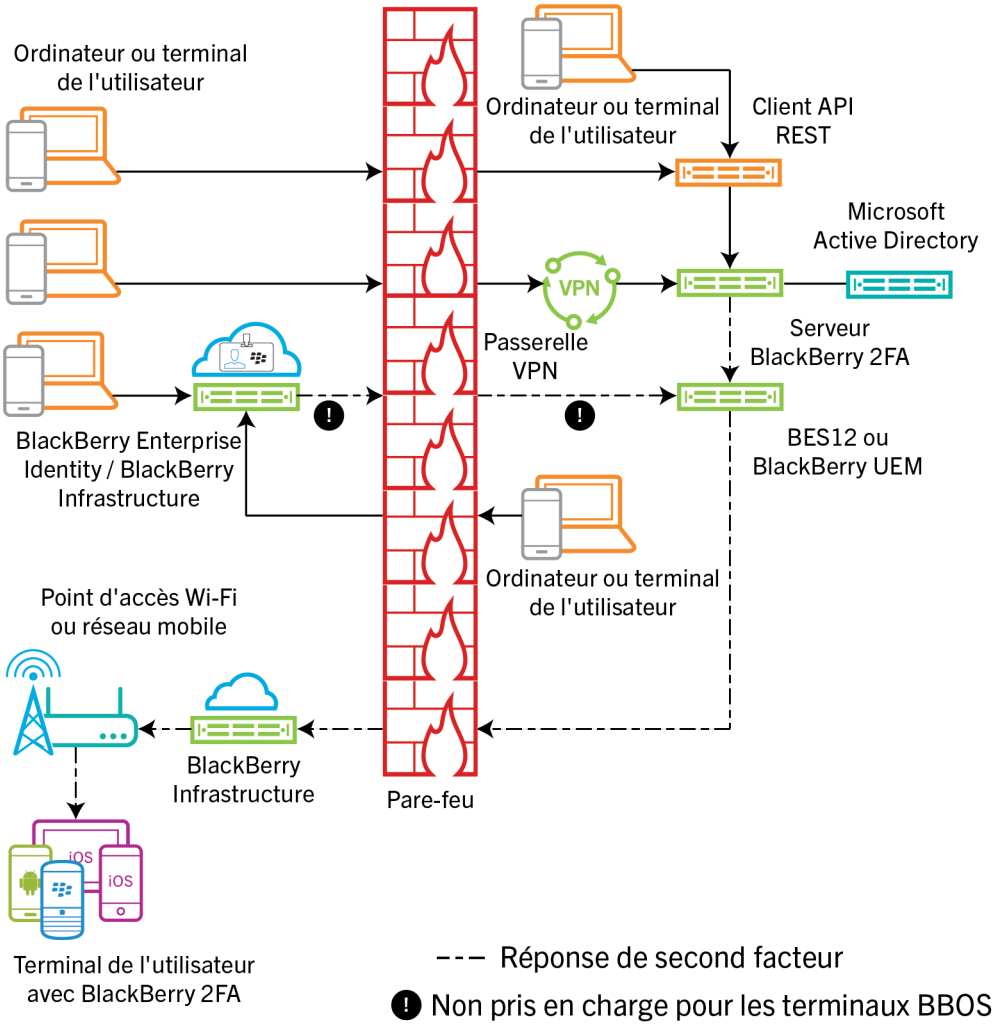
Architecture : BlackBerry 2FA



Composant	Description
Ordinateur ou terminal de l'utilisateur	L'ordinateur ou le terminal d'un utilisateur est tout ordinateur ou terminal, à l'intérieur ou à l'extérieur d'un pare-feu, qui sert à se connecter à une ressource nécessitant l'authentification à deux facteurs.
Serveur BlackBerry 2FA	Le serveur BlackBerry 2FA se connecte au module BlackBerry UEM pour détecter les terminaux associés à un utilisateur et pour envoyer des demandes d'authentification à l'application BlackBerry 2FA installée sur les terminaux.
Passerelle VPN (facultative)	La passerelle VPN est un ordinateur qui accepte les connexions VPN au réseau de votre organisation. **Remarque :** Cette fonctionnalité requiert le serveur BlackBerry 2FA.
Client API REST (facultatif)	Le client API REST est un service sur site défini par l'utilisateur, qui authentifie les utilisateurs qui y accèdent par l'intermédiaire de l'API REST du serveur BlackBerry 2FA. **Remarque :** Cette fonctionnalité requiert le serveur BlackBerry 2FA.
BlackBerry Enterprise Identity (facultatif)	BlackBerry Enterprise Identity fournit l'authentification unique (SSO) à des services en nuage, tels que Box, Salesforce et G Suite. Enterprise Identity se connecte directement au service BlackBerry 2FA dans BlackBerry UEM ou BlackBerry UEM Cloud.

Composant	Description
BES12 ou BlackBerry UEM, BlackBerry UEM Cloud	BlackBerry UEM gère également la configuration des utilisateurs BlackBerry 2FA via le profil BlackBerry 2FA et l'utilisation de jetons de mot de passe à usage unique (OTP).
Terminal d'utilisateur avec BlackBerry 2FA	Pour les terminaux iOS et Android, BlackBerry 2FA est inclus dans BlackBerry UEM Client. Pour les terminaux BlackBerry 10, les utilisateurs installent l'application BlackBerry 2FA.

Demandes d'authentification via BlackBerry UEM



Pour initier une demande d'authentification, un utilisateur doit effectuer l'une des opérations suivantes :

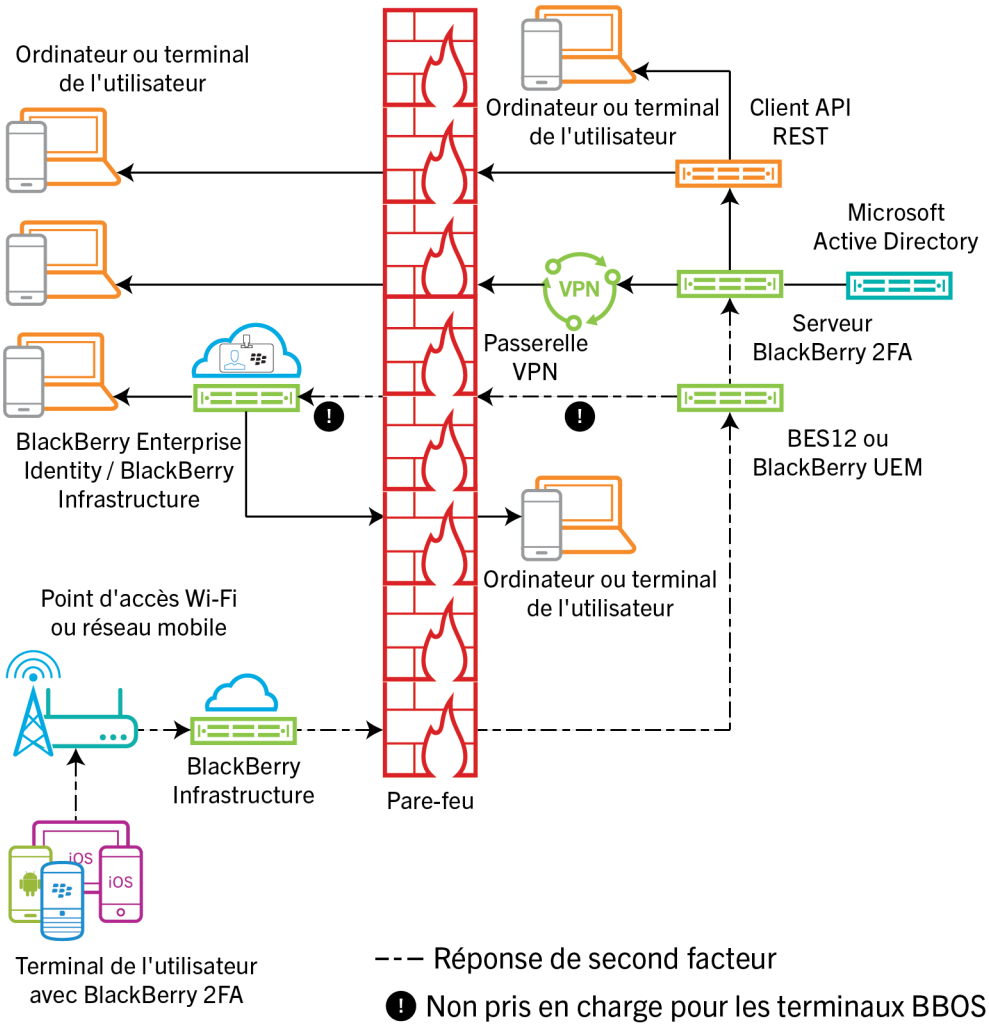
- Accéder à l'interface de connexion pour un service personnalisé sur un ordinateur ou terminal professionnel et saisir ses informations de connexion

- Accéder à l'interface de connexion pour un service personnalisé sur un ordinateur ou terminal non professionnel et saisir ses informations de connexion
- Ouvrir un client VPN sur un ordinateur ou terminal non professionnel et saisir ses informations de connexion
- Accéder à l'interface de connexion d'un service configuré pour utiliser BlackBerry Enterprise Identity pour l'authentification sur un ordinateur ou terminal non professionnel et saisir ses informations de connexion
- Accéder à l'interface de connexion d'un service configuré pour utiliser BlackBerry Enterprise Identity pour l'authentification sur un ordinateur ou terminal professionnel et saisir ses informations de connexion

L'utilisateur reçoit un message sur son terminal l'invitant à confirmer qu'il souhaite s'authentifier. En fonction des options d'authentification configurées pour l'utilisateur, ce dernier devra peut-être saisir le mot de passe de son terminal ou de son conteneur sécurisé avant de pouvoir reconnaitre le message.

Le schéma n'illustre pas le flux de demandes d'authentification qui utilisent des jetons de mot de passe à usage unique (OTP).

Réponses d'authentification via BlackBerry UEM

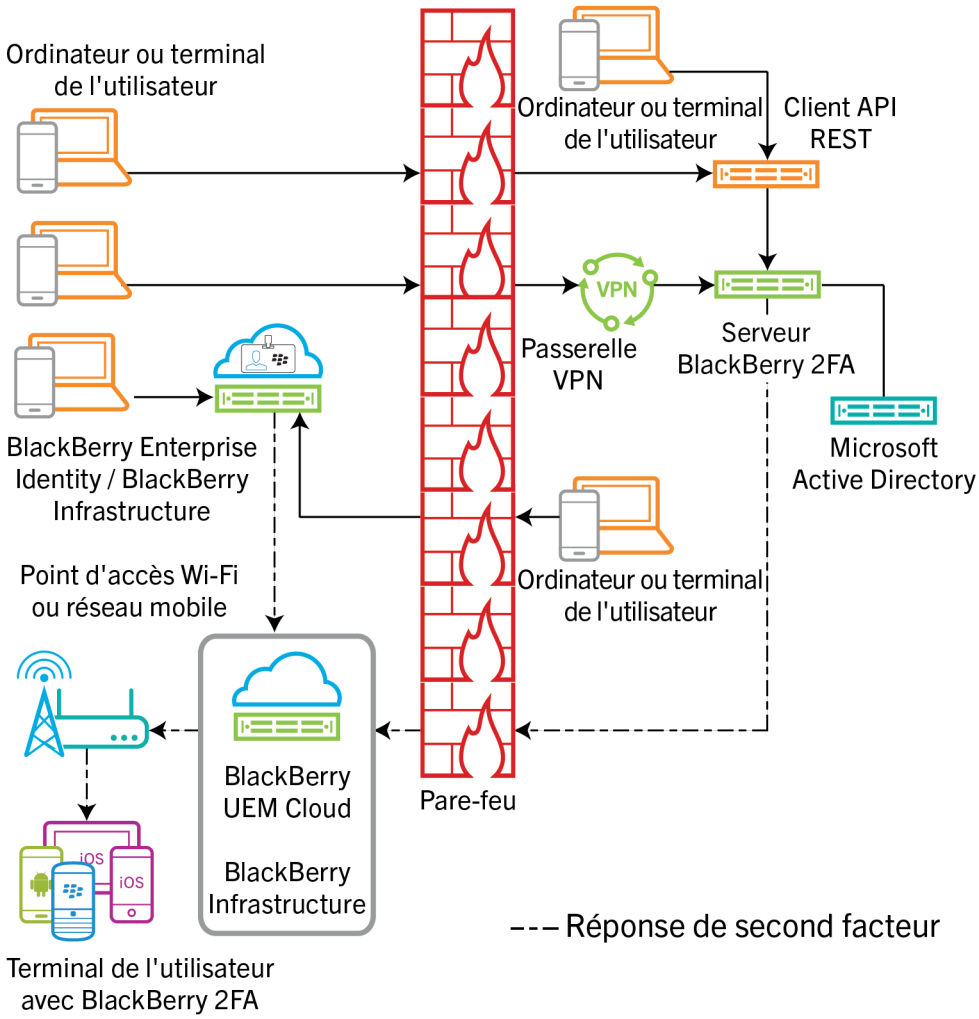


Dans toutes les réponses affichées, l'utilisateur confirme la demande d'authentification sur son terminal et la réponse retourne à BlackBerry Enterprise Identity ou au serveur BlackBerry 2FA. Le mot de passe du répertoire

de l'utilisateur est vérifié si les options d'authentification de l'utilisateur l'exigent. Après la vérification, l'utilisateur reçoit un message sur son terminal indiquant que la réponse à la demande a été envoyée avec succès.

Le schéma n'illustre pas le flux de données d'authentifications qui utilisent des jetons de mot de passe à usage unique (OTP).

Demandes d'authentification via BlackBerry UEM Cloud



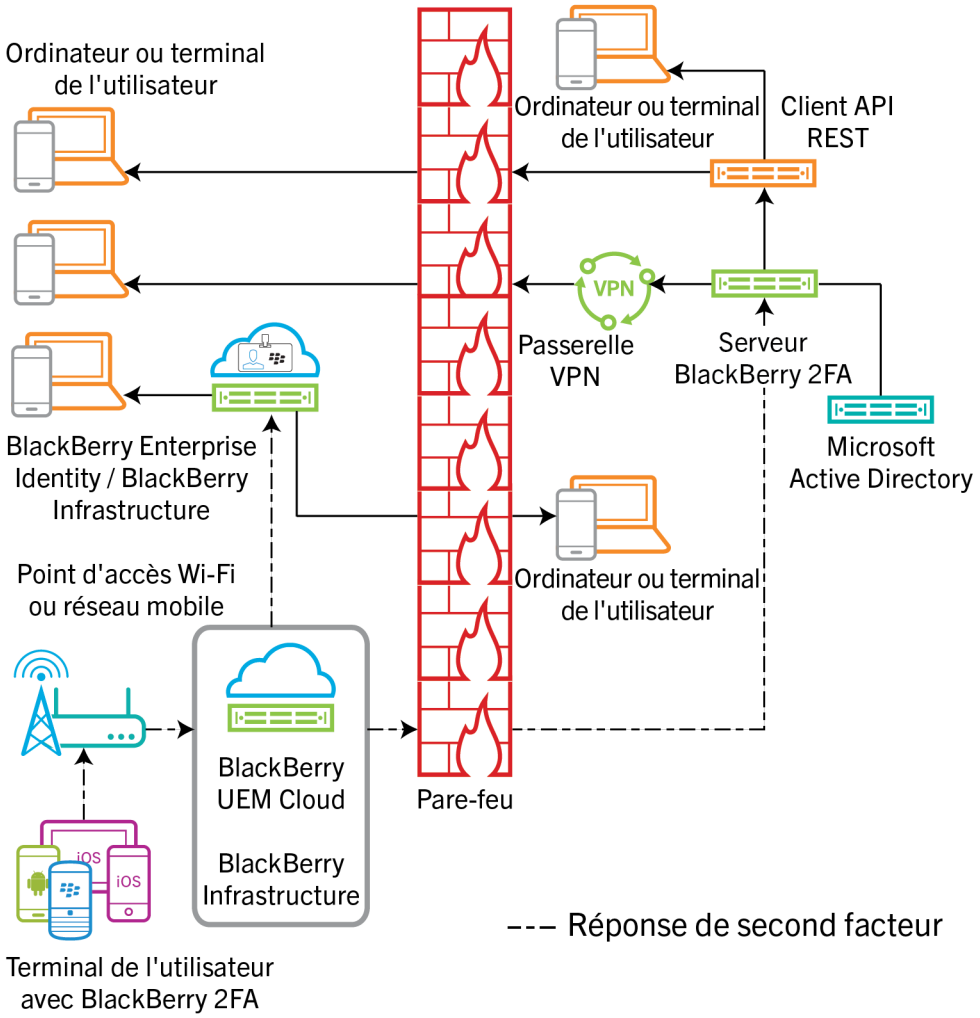
Pour initier une demande d'authentification, un utilisateur doit effectuer l'une des opérations suivantes :

- Accéder à l'interface de connexion d'un service configuré pour utiliser BlackBerry Enterprise Identity pour l'authentification sur un ordinateur ou terminal non professionnel et saisir ses informations de connexion
- Accéder à l'interface de connexion d'un service configuré pour utiliser BlackBerry Enterprise Identity pour l'authentification sur un ordinateur ou terminal professionnel et saisir ses informations de connexion

L'utilisateur reçoit un message sur son terminal l'invitant à confirmer qu'il souhaite s'authentifier. En fonction des options d'authentification configurées pour l'utilisateur, ce dernier devra peut-être saisir le mot de passe de son terminal ou de son conteneur sécurisé avant de pouvoir reconnaitre le message.

Le schéma n'illustre pas le flux de demandes d'authentification qui utilisent des jetons de mot de passe à usage unique (OTP).

Réponses d'authentification via BlackBerry UEM Cloud



Dans toutes les réponses affichées, l'utilisateur confirme la demande d'authentification sur son terminal et la réponse retourne à BlackBerry Enterprise Identity. Le mot de passe du répertoire de l'utilisateur est vérifié si les options d'authentification de l'utilisateur l'exigent. Après la vérification, l'utilisateur reçoit un message sur son terminal indiquant que la réponse à la demande a été envoyée avec succès.

Le schéma n'illustre pas le flux de données d'authentifications qui utilisent des jetons de mot de passe à usage unique (OTP).

Mise à niveau de BlackBerry UEM

Si vous mettez à niveau BlackBerry UEM et que vous utilisez un serveur BlackBerry 2FA, après la mise à niveau, vous devez redémarrer le service BlackBerry 2FA sur le serveur 2FA. Par exemple, si vous effectuez la mise à niveau à partir de la version 12.6 à 12.7 de BlackBerry UEM et que vous exécutez le serveur BlackBerry 2FA 2.5, redémarrez le service BlackBerry 2FA sur le serveur 2FA.

Pour obtenir les dernières informations de compatibilité, reportez-vous à la matrice de compatibilité du serveur BlackBerry 2FA.

Profils BlackBerry 2FA

Vous pouvez utiliser un profil BlackBerry 2FA pour activer l'authentification pour vos utilisateurs. Pour utiliser la dernière version de BlackBerry 2FA et ses fonctionnalités associées, comme la prise en charge de jetons matériels OTP, la prise en charge de jetons logiciels OTP, l'authentification directe BlackBerry 2FA, la pré-authentification BlackBerry 2FA et la résolution autonome, le profil BlackBerry 2FA doit être attribué à vos utilisateurs. Pour obtenir des informations sur l'utilisation du profil BlackBerry 2FA, reportez-vous aux sections Créer ou modifier un profil BlackBerry 2FA dans BlackBerry UEM version 12.8 ou antérieure et Attribuer un profil BlackBerry 2FA à un utilisateur. Pour plus d'informations sur l'utilisation de BlackBerry 2FA dans BlackBerry UEM, reportez-vous à la section Étapes pour gérer BlackBerry 2FA dans BlackBerry UEM .

BlackBerry 2FA pour les terminaux gérés par BlackBerry UEM

Vous pouvez activer des terminaux dans BlackBerry UEM afin de pouvoir les gérer et utiliser BlackBerry 2FA. Une tâche d'activation unique fournit au terminal le contrôle MDM et BlackBerry 2FA, ce qui simplifie la gestion du terminal à la fois pour les utilisateurs et les administrateurs.

N'importe quel profil d'activation pris en charge par BlackBerry UEM permet l'utilisation de BlackBerry 2FA. Pour plus d'informations sur l'utilisation de BlackBerry 2FA dans BlackBerry UEM, reportez-vous au contenu relatif à l'administration de BlackBerry 2FA.

BlackBerry 2FA pour les terminaux non gérés par BlackBerry UEM

Si la gestion BlackBerry UEM n'est pas possible ou si un terminal est déjà géré par une autre solution MDM, vous pouvez activer des terminaux avec BlackBerry UEM pour qu'ils puissent utiliser uniquement BlackBerry 2FA.

Les terminaux activés de cette façon ne sont pas gérés par BlackBerry UEM. Aucun espace Travail n'est créé sur les terminaux, aucun contrôle administratif du terminal n'est établi, aucune sécurité n'est ajoutée pour les données professionnelles et les données personnelles des utilisateurs restent privées.

Cette option est disponible pour les terminaux iOS et Android uniquement. Pour plus d'informations sur l'utilisation de BlackBerry 2FA dans BlackBerry UEM, reportez-vous au contenu relatif à l'administration de BlackBerry 2FA.

Jetons OTP

BlackBerry UEM prend en charge l'utilisation de jetons de mot de passe à usage unique (OTP) via le service BlackBerry 2FA. Les jetons OTP constituent une fonctionnalité d'authentification sécurisée pour les utilisateurs qui ne disposent pas d'un terminal mobile ou dont le terminal ne dispose pas d'une connectivité suffisante pour prendre en charge les notifications en temps réel BlackBerry 2FA. En cas d'utilisation d'un OTP au lieu d'une notification du terminal comme authentification de type second facteur, l'OTP est fourni dans le même canal que le mot de passe de l'utilisateur et son terminal mobile n'est pas signalé.

Vous pouvez saisir le code OTP avec le nom d'utilisateur ou le mot de passe.

- Lorsque vous utilisez un code OTP avec le nom d'utilisateur, vous devez saisir le nom d'utilisateur suivi d'une virgule (,) et du code OTP, sans espaces. Par exemple, si le nom d'utilisateur est « janedoe » et le code « 555123 », vous devez saisir « janedoe,555123 ». Cette méthode permet aux utilisateurs de vérifier facilement le code qu'ils ont saisi.

- Lorsque vous utilisez un code OTP avec mot de passe, le code précède le mot de passe de l'utilisateur. Par exemple, si le code est « 555123 » et le mot de passe « AbCdeF », il doit être saisi « 555123AbCdeF ».

Jetons logiciels

Les jetons logiciels OTP des utilisateurs s'activent dans le profil BlackBerry 2FA que vous leur avez attribué. Vous pouvez trouver le jeton logiciel dans l'application BlackBerry UEM Client en faisant glisser votre doigt sur son écran d'accueil.

Jetons matériels

Pour gérer des jetons matériels OTP dans BlackBerry UEM, un profil BlackBerry 2FA doit avoir été attribué à l'utilisateur.

Pour plus d'informations sur les derniers jetons matériels en date pris en charge, reportez-vous aux tableaux de compatibilité du serveur BlackBerry 2FA.

Pré-authentification et résolution autonome

La pré-authentification et la résolution autonome sont des fonctionnalités de BlackBerry 2FA qui permettent aux utilisateurs de s'authentifier afin d'accéder aux ressources de votre entreprise pendant une période prédéfinie avec un seul facteur. Ces fonctionnalités sont activées et configurées indépendamment.

La pré-authentification doit être utilisée lorsque l'utilisateur s'attend à ne pas pouvoir accéder au terminal ou à ne pas pouvoir bénéficier d'une couverture réseau pendant une courte période (par exemple, à bord d'un avion). Les utilisateurs peuvent demander la pré-authentification à partir de leur terminal ou les administrateurs peuvent l'activer via la console de gestion BlackBerry UEM. BlackBerry recommande d'utiliser plutôt la fonctionnalité logicielle de mot de passe à usage unique, si possible, car elle conserve une sécurité à deux facteurs intégrale, même si elle est moins intuitive.

La résolution autonome doit être utilisée lorsqu'un utilisateur a perdu son terminal ou ne parvient pas à accéder à son terminal pendant une longue période, c'est-à-dire une journée entière ou plus (par exemple, l'utilisateur a perdu son terminal et attend un terminal de rechange). Les utilisateurs peuvent accéder à la fonctionnalité de résolution autonome à partir de BlackBerry UEM Self-Service, ce qui signifie qu'elle peut être activée uniquement si l'utilisateur est connecté au réseau de l'organisation.

Authentification directe

Vous pouvez activer la fonction d'authentification directe BlackBerry 2FA de sorte que lorsque les utilisateurs souhaitent s'authentifier auprès des ressources de votre entreprise, ils commencent le processus d'authentification à partir de leurs terminaux au lieu de recevoir un message leur demandant une confirmation sans utilisation de mot de passe à usage unique. Lorsque vous activez la fonction d'authentification directe pour les utilisateurs, ces derniers doivent utiliser le mot de passe de leur répertoire pour se connecter aux ressources de votre entreprise dans le délai défini par vos soins.

Les utilisateurs peuvent accéder à la fonctionnalité d'authentification directe depuis BlackBerry UEM Client sur les terminaux Android et iOS et l'application BlackBerry 2FA sur les terminaux BlackBerry 10.

Étapes pour gérer BlackBerry 2FA dans BlackBerry UEM

Pour utiliser BlackBerry UEM afin de gérer BlackBerry 2FA, vous effectuez les actions suivantes :

Étape	Action
1	Vérifiez que votre environnement répond à la configuration de terminaux et serveur requise. Pour plus d'informations, reportez-vous à Configuration système requise : BlackBerry 2FA.
2	Vous pouvez également installer et configurer le serveur BlackBerry 2FA. Pour plus d'informations, consultez le contenu relatif à l' installation et à la mise à niveau de .
3	Créer un utilisateur.
4	Attribuer l'application BlackBerry 2FA à des terminaux BlackBerry 10.
5	Créer ou modifier un profil BlackBerry 2FA dans BlackBerry UEM version 12.8 ou antérieure ou Créer ou modifier un profil BlackBerry 2FA dans BlackBerry UEM Cloud ou BlackBerry UEM version 12.9 ou ultérieure.
6	Attribuer un profil BlackBerry 2FA à un utilisateur.
7	Sinon, Créer un profil d'activation pour enregistrer des terminaux non gérés avec BlackBerry 2FA.
8	Sinon, Attribuer un profil d'activation d'enregistrement uniquement à un utilisateur disposant d'un terminal non géré.
9	Activer un terminal BlackBerry 10.
10	Activer un terminal iOS.
11	Activer un terminal Android.
12	Configurer ou annuler la pré-authentification.
13	Vous pouvez également configurer BlackBerry UEM pour l'utilisation de jetons de mot de passe à usage unique (OTP). Pour plus d'informations, reportez-vous à Étapes à suivre pour gérer les jetons matériels de mot de passe à usage unique.

Configuration système requise : BlackBerry 2FA

Avant de pouvoir utiliser BlackBerry UEM pour gérer BlackBerry 2FA, vous devez vous assurer que les exigences de configuration suivantes sont satisfaites :

Élément	Configuration requise
BlackBerry UEM ou BlackBerry UEM Cloud	Une des licences suivantes : • BlackBerry UEM version 12.6 ou ultérieure • BlackBerry UEM Cloud Pour obtenir des informations sur l'installation de BlackBerry UEM 12.6 ou version ultérieure, reportez-vous au contenu relatif à l'installation et à la mise à niveau de BlackBerry UEM.
Serveur BlackBerry 2FA	• Version 2.0 ou ultérieure (version 2.5 pour une intégration complète de toutes les nouvelles fonctionnalités de BlackBerry UEM, y compris les jetons OTP) Pour en savoir plus sur la configuration requise, consultez le contenu relatif à la matrice de compatibilité de BlackBerry 2FA. **Remarque :** Pour gérer le serveur BlackBerry 2FA à partir de la console de gestion BlackBerry UEM, le serveur BlackBerry 2FA version 2.5 est requis.
Licences BlackBerry 2FA	• BlackBerry 2FA est inclus dans BlackBerry Enterprise Mobility Suite - Application Edition et BlackBerry Enterprise Mobility Suite - Content Edition, et peut également être acheté séparément. • BlackBerry 2FA est inclus dans BlackBerry Enterprise Mobility Suite - Collaboration Edition pour authentification auprès des produits d'entreprise propriétaires Microsoft Office 365 et BlackBerry uniquement. • BlackBerry 2FA est inclus dans toutes les licences autonomes BlackBerry Workspaces pour authentification auprès de Workspaces uniquement. • Contactez votre représentant de compte BlackBerry pour obtenir les informations les plus récentes sur l'emballage, les tarifs et les licences.
BlackBerry 10	• Toutes les versions. Pour plus d'informations, reportez-vous au contenu relatif à la matrice de compatibilité de BlackBerry 2FA.
iOS	• iOS 8 et versions ultérieures. Pour plus d'informations, reportez-vous au contenu relatif à la matrice de compatibilité de BlackBerry 2FA. • Dernière version de l'application BlackBerry UEM Client installée. Pour plus d'informations, reportez-vous au contenu relatif à l'administration de BlackBerry UEM.
Android	• Android 4.0.x et versions ultérieures. Pour plus d'informations, reportez-vous au contenu relatif à la matrice de compatibilité de BlackBerry 2FA. • Dernière version de l'application BlackBerry UEM Client installée. Pour plus d'informations, reportez-vous au contenu relatif à l'administration de BlackBerry UEM.

Élément	Configuration requise
Licences de terminal	Aucune licence n'est requise pour les terminaux qui utilisent BlackBerry 2FA mais qui ne sont pas gérés par BlackBerry UEM.

Créer un utilisateur

Chaque utilisateur BlackBerry 2FA doit exister en tant qu'utilisateur dans BlackBerry UEM. Effectuez l'une des opérations suivantes :

- Si l'utilisateur est déjà présent dans BlackBerry UEM, suivez les instructions pour définir un mot de passe d'activation et envoyer un e-mail d'activation dans le contenu relatif à l'administration de BlackBerry UEM.
- Si l'utilisateur n'est pas encore présent dans BlackBerry UEM, suivez ces étapes pour en créer un et lui envoyer un mot de passe d'activation.

Pour la version avancée de cette tâche, suivez les instructions de création d'un compte utilisateur dans le contenu relatif à l'administration de BlackBerry UEM.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Utilisateurs** sur la barre de menus.
2. Dans le volet de gauche, cliquez sur **Ajouter un utilisateur**.
3. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Ajouter un utilisateur de répertoire.	**a.** Dans le champ de recherche de l'onglet **Répertoire d'entreprise**, spécifiez les critères de recherche de l'utilisateur d'annuaire que vous souhaitez ajouter. Vous pouvez effectuer une recherche par nom, prénom, nom d'affichage, nom d'utilisateur ou adresse électronique. **b.** Cliquez sur . **c.** Dans les résultats de la recherche, sélectionnez le compte d'utilisateur.
Ajouter un utilisateur local.	**a.** Cliquez sur l'onglet **Local**. **b.** Saisissez le **Prénom** et le **Nom** du compte d'utilisateur. **c.** Dans le champ **Nom d'affichage**, apportez des modifications, si nécessaire. Le nom d'affichage est automatiquement configuré avec le prénom et le nom que vous avez spécifiés. **d.** Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur unique pour le compte d'utilisateur. **e.** Dans le champ **Adresse électronique**, saisissez une adresse électronique de contact pour le compte d'utilisateur. Une adresse électronique est obligatoire pour le compte d'utilisateur, lorsque vous activez un service comme la gestion de terminal ou BlackBerry Workspaces. **f.** Dans le champ **Mot de passe de la console**, saisissez un mot de passe pour BlackBerry UEM Self-Service. Si un rôle d'administrateur est attribué à l'utilisateur, il peut également utiliser le mot de passe pour accéder à la console de gestion.

4. Effectuez l'une des tâches suivantes :

Tâche	Étapes
Générer automatiquement un mot de passe d'activation pour l'utilisateur et envoyer un e-mail d'activation.	a. Sélectionnez l'option **Générer automatiquement le mot de passe d'activation du terminal et envoyer un e-mail contenant des instructions d'activation**. b. Dans le champ **Expiration de la période d'activation**, spécifiez le nombre de minutes, d'heures ou de jours pendant lesquels l'utilisateur est autorisé à activer un terminal avant que son mot de passe d'activation expire. c. Dans la liste déroulante **Modèle d'e-mail d'activation**, cliquez sur un modèle à utiliser pour l'e-mail d'activation.
Définir un mot de passe d'activation pour l'utilisateur et, éventuellement, envoyer un e-mail d'activation.	a. Sélectionnez l'option **Définir le mot de passe d'activation du terminal**. b. Saisissez un mot de passe d'activation. c. Dans le champ **Expiration de la période d'activation**, spécifiez le nombre de minutes, d'heures ou de jours pendant lesquels l'utilisateur est autorisé à activer un terminal avant que son mot de passe d'activation expire. d. Effectuez l'une des opérations suivantes : 1. Pour envoyer des instructions d'activation à l'utilisateur, dans la liste déroulante **Modèle d'e-mail d'activation**, cliquez sur un modèle à utiliser pour l'e-mail d'activation. 2. Si vous ne souhaitez pas envoyer les instructions d'activation à l'utilisateur, décochez la case **Envoyer un e-mail contenant le mot de passe d'activation et les instructions**. Vous devez communiquer le mot de passe d'activation à l'utilisateur.
Ne pas définir de mot de passe d'activation pour l'utilisateur.	a. Sélectionnez l'option **Ne pas définir de mot de passe d'activation du terminal**. Vous pouvez définir un mot de passe d'activation et envoyer un e-mail d'activation ultérieurement.

5. Si vous utilisez des variables personnalisées, développez **Variables personnalisées** et spécifiez les valeurs appropriées pour les variables que vous avez définies.
6. Effectuez l'une des opérations suivantes :
   - Pour enregistrer l'utilisateur, cliquez sur **Enregistrer**.
   - Pour enregistrer l'utilisateur et créer un autre compte d'utilisateur, cliquez sur **Enregistrer et ajouter nouveau**.

Attribuer l'application BlackBerry 2FA à des terminaux BlackBerry 10

Vous devez effectuer la tâche suivante pour attribuer l'application à des terminaux BlackBerry 10 lorsque vous utilisez BlackBerry UEM. Pour plus d'informations sur la gestion des applications, consultez le contenu relatif à l'administration de BlackBerry UEM.

1. Téléchargez l'application à partir de https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B et copiez le fichier .bar dans un emplacement accessible par la console de gestion BlackBerry UEM.

2. Si nécessaire, utilisez la console de gestion BlackBerry UEM pour spécifier un emplacement réseau partagé pour les applications internes.
3. Dans la console de gestion BlackBerry UEM, ajoutez le fichier .bar en tant qu'application interne.
4. Dans la console de gestion BlackBerry UEM, attribuez l'application à des utilisateurs ou à des groupes.

L'application est installée automatiquement sur n'importe quel terminal BlackBerry 10 que l'utilisateur active avec un espace Travail.

Créer ou modifier un profil BlackBerry 2FA dans BlackBerry UEM version 12.8 ou antérieure

Pour utiliser BlackBerry 2FA, vous devez créer un profil BlackBerry 2FA et l'attribuer à des utilisateurs.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions** > **BlackBerry 2FA**.
3. Effectuez l'une des opérations suivantes :
   - Pour créer un profil, cliquez sur +.
   - Pour modifier un profil, cliquez sur le nom du profil que vous souhaitez modifier et cliquez sur .
4. Attribuez un nom au profil BlackBerry 2FA.
5. Vous pouvez également ajouter une description au profil BlackBerry 2FA.
6. Sélectionnez une option d'authentification :
   a) Sélectionnez **Authentification à deux facteurs** si vous créez un profil BlackBerry 2FA standard.
   b) Sélectionnez **Authentification à un seul facteur avec mot de passe d'entreprise** si vous créez un profil pour des utilisateurs qui ne disposent pas de terminal mais qui ont besoin d'accéder aux ressources de votre organisation. Cette option est moins sécurisée, car l'utilisateur fournit uniquement un mot de passe du répertoire lorsqu'il demande l'authentification et aucune demande de confirmation d'authentification n'est envoyée. Les jetons de mot de passe à usage unique (OTP) ne sont pas pris en charge avec cette option.
7. Sélectionnez un mot de passe à utiliser avec une invite :
   a) Sélectionnez **Mot de passe d'entreprise** si vous créez un profil pour des utilisateurs qui doivent au préalable fournir leur mot de passe de répertoire lorsqu'ils demandent l'authentification, puis reçoivent une demande de confirmation sur leur terminal.
   b) Sélectionnez **Mot de passe passif du terminal** si vous créez un profil pour les utilisateurs BlackBerry 10 qui doivent recevoir une invite passive pour fournir leur mot de passe de l'espace Travail pour déverrouiller ce dernier, puis recevoir une demande de confirmation d'authentification sur leur terminal. L'invite passive signifie que l'utilisateur n'est pas tenu de fournir un mot de passe de l'espace Travail si celui-ci est déjà déverrouillé lorsque l'utilisateur demande une authentification.
   c) Sélectionnez **Mot de passe actif du terminal** si vous créez un profil pour les utilisateurs BlackBerry 10 qui doivent recevoir une invite active pour fournir leur mot de passe de l'espace Travail pour déverrouiller ce dernier, puis recevoir une demande de confirmation d'authentification sur leur terminal. L'invite active signifie que l'utilisateur est tenu de fournir un mot de passe de l'espace Travail si l'espace Travail du terminal est déjà déverrouillé lorsque l'utilisateur demande une authentification.
8. Si vous le souhaitez, si vous utilisez la stratégie d'authentification **Mot de passe d'entreprise**, effectuez l'une des opérations suivantes :
   a) Pour autoriser les utilisateurs à utiliser des mots de passe à usage unique dans l'application BlackBerry UEM Client, sélectionnez **Autoriser les jetons de mot de passe à usage unique**. Spécifiez la longueur des mots de passe à usage unique générés.

b) Pour autoriser les utilisateurs à demander l'authentification directe, sélectionnez **Autoriser l'authentification directe depuis le terminal de l'utilisateur**. Spécifiez la durée, en secondes, pendant laquelle les utilisateurs peuvent terminer l'authentification à deux facteurs après l'avoir démarrée sur leur terminal mobile. Le paramètre maximal est 180.
c) Pour autoriser les utilisateurs à définir une période de résolution autonome, sélectionnez **Autoriser la résolution autonome à partir de BlackBerry UEM Self-Service**. Spécifiez la durée maximale par défaut (en heures) pendant laquelle les utilisateurs peuvent accéder aux ressources de votre organisation sans devoir répondre à une invite de confirmation sur leur terminal.
d) Dans le but de permettre aux utilisateurs de définir une période de pré-authentification, sélectionnez **Autoriser la pré-authentification depuis le terminal de l'utilisateur**. Spécifiez la durée maximale par défaut (en heures) pendant laquelle les utilisateurs peuvent accéder aux ressources de votre entreprise sans devoir répondre à une invite de confirmation sur leur terminal (l'invite n'apparaît pas).

9. Cliquez sur **Ajouter** ou **Enregistrer**.

Créer ou modifier un profil BlackBerry 2FA dans BlackBerry UEM Cloud ou BlackBerry UEM version 12.9 ou ultérieure

Pour utiliser BlackBerry 2FA, vous devez créer un profil BlackBerry 2FA et l'attribuer à des utilisateurs.

1. Sur la barre de menus, cliquez sur **Stratégies et profils**.
2. Cliquez sur **Réseaux et connexions** > **BlackBerry 2FA**.
3. Effectuez l'une des opérations suivantes :
   - Pour créer un profil, cliquez sur +.
   - Pour modifier un profil, cliquez sur le nom du profil que vous souhaitez modifier et cliquez sur .
4. Attribuez un nom au profil BlackBerry 2FA.
5. Vous pouvez également ajouter une description au profil BlackBerry 2FA.
6. Effectuez l'une des opérations suivantes :
   a) Sélectionnez **Authentification avec BlackBerry 2FA** si vous créez un profil BlackBerry 2FA standard.
   b) Sélectionnez **Authentification avec mot de passe d'entreprise seulement** si vous créez un profil pour des utilisateurs qui ne disposent pas de terminal mais qui ont besoin d'accéder aux ressources de votre organisation. Cette option est moins sécurisée, car l'utilisateur fournit uniquement un mot de passe du répertoire lorsqu'il demande l'authentification et aucune demande de confirmation d'authentification n'est envoyée. Les jetons de mot de passe à usage unique (OTP) ne sont pas pris en charge avec cette option.
7. Si vous avez sélectionné le mode d'authentification « Authentifier avec BlackBerry 2FA », configurez les paramètres suivants :

Paramètre	Description
Autoriser l'authentification Push	Ce paramètre indique si les utilisateurs peuvent s'authentifier à l'aide de la demande de confirmation 2FA sur leur terminal.
Mot de passe d'entreprise requis	Ce paramètre indique si les utilisateurs doivent fournir leur mot de passe d'entreprise lors de la connexion aux ressources de votre entreprise. Une fois qu'un utilisateur a saisi son mot de passe, il est invité à s'authentifier sur son terminal.

Paramètre	Description
	Ce paramètre est valide uniquement si l'option Activer l'authentification Push est sélectionnée.
Autoriser la pré-authentification à partir de terminaux mobiles	Ce paramètre indique si les utilisateurs peuvent se servir de la fonction pré-authentification pour s'authentifier auprès des ressources de votre entreprise pendant une courte période prédéterminée. Si vous sélectionnez cette option, la fonction est disponible pour les utilisateurs dans l'écran d'accueil de l'application BlackBerry UEM Client. Spécifier la durée maximale par défaut (en heures) après laquelle les utilisateurs reçoivent une demande de confirmation d'authentification sur leur terminal pour accéder aux ressources de votre entreprise. Ce paramètre est valide uniquement si les options Autoriser l'authentification Push et Mot de passe d'entreprise requis sont sélectionnées.
Mot de passe du terminal requis si le terminal est verrouillé	Ce paramètre indique si les utilisateurs doivent déverrouiller leur terminal avant de pouvoir répondre à la demande de confirmation d'authentification sur le terminal. Ce paramètre est valide uniquement si l'option Activer l'authentification Push est sélectionnée.
Nouvelle saisie du mot de passe du terminal requise même si le terminal est déjà déverrouillé (terminaux BlackBerry 10 uniquement)	Ce paramètre indique si les utilisateurs de terminaux BlackBerry 10 doivent saisir le mot de passe, même si le terminal est déjà déverrouillé, avant de répondre à la demande de confirmation d'authentification sur le terminal. Ce paramètre est valide uniquement si les options Autoriser l'authentification Push et Mot de passe du terminal requis sont sélectionnées lorsque le terminal est verrouillé.
Autoriser l'authentification directe à partir de terminaux mobiles	Ce paramètre indique si les utilisateurs peuvent utiliser la fonction Authentification directe pour démarrer le processus d'authentification sur leur terminal mobile. Si vous sélectionnez cette option, la fonction est disponible pour les utilisateurs dans l'écran d'accueil de l'application BlackBerry UEM Client. Vous devez spécifier la durée (en secondes) au cours de laquelle les utilisateurs doivent terminer le processus d'authentification à deux facteurs. La

Paramètre	Description
	valeur par défaut est « 120 » et la valeur maximale est « 180. » Ce paramètre est valide uniquement si l'option Activer l'authentification Push est sélectionnée.
Autoriser l'authentification mot de passe à usage unique	Ce paramètre indique si les utilisateurs peuvent utiliser les codes de mot de passe à usage unique comme second facteur d'authentification.
Mot de passe d'entreprise requis	Ce paramètre spécifie si l'utilisateur doit saisir le mot de passe de son répertoire avec le code mot de passe à usage unique. Ce paramètre est valide uniquement si l'option Activer l'authentification mot de passe à usage unique est sélectionnée.
Autoriser la génération de mot de passe à usage unique sur les terminaux mobiles	Ce paramètre indique s'il faut générer des codes mot de passe à usage unique sur le terminal mobile. Si vous sélectionnez cette option, les utilisateurs peuvent utiliser des codes mot de passe à usage unique qui s'affichent dans l'écran d'accueil de l'application BlackBerry UEM Client. Spécifier la longueur des codes mot de passe à usage unique que vous voulez générer dans le UEM Client. La longueur par défaut est « 6. » Ce paramètre est valide uniquement si l'option Activer l'authentification mot de passe à usage unique est sélectionnée.
Accepter les jetons matériels mot de passe à usage unique	Ce paramètre indique si les utilisateurs ont la possibilité d'utiliser des jetons matériels mot de passe à usage unique. Si vous sélectionnez cette option, les utilisateurs peuvent utiliser les codes mot de passe à usage unique sur les jetons matériels qui leur ont été attribués. Ce paramètre est valide uniquement si l'option Activer l'authentification mot de passe à usage unique est sélectionnée.
Autoriser Résolution autonome à partir de BlackBerry UEM Self-Service	Ce paramètre indique si les utilisateurs peuvent se servir de la fonction Résolution autonome pour s'authentifier aux ressources de votre entreprise pour une période prédéterminée. Si vous sélectionnez cette option, les utilisateurs peuvent accéder à la fonction Résolution autonome à partir de BlackBerry UEM Self-Service, accessible aux utilisateurs uniquement s'ils sont connectés au réseau de l'entreprise.

Paramètre	Description
	Spécifier la durée maximale par défaut (en heures) après laquelle les utilisateurs reçoivent une demande de confirmation d'authentification sur leur terminal pour accéder aux ressources de votre entreprise.

8. Cliquez sur **Ajouter** ou **Enregistrer**.

Attribuer un profil BlackBerry 2FA à un utilisateur

Un utilisateur doit avoir un profil BlackBerry 2FA pour utiliser BlackBerry 2FA.

Avant de commencer :

- Créer ou modifier un profil BlackBerry 2FA dans BlackBerry UEM version 12.8 ou antérieure.
- Créer ou modifier un profil BlackBerry 2FA dans BlackBerry UEM Cloud ou BlackBerry UEM version 12.9 ou ultérieure.

1. Dans la console de gestion, cliquez sur **Utilisateurs** sur la barre de menu.
2. Recherchez un utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom de l'utilisateur.
4. Dans la section **Stratégie informatique et profils**, cliquez sur +.
5. Cliquez sur **BlackBerry 2FA**.
6. Dans la liste déroulante **Profil BlackBerry 2FA**, cliquez sur un profil BlackBerry 2FA.
7. Si le type de profil que vous avez sélectionné à l'étape 6 est déjà directement attribué à l'utilisateur, cliquez sur **Remplacer**. Sinon, cliquez sur **Attribuer**.

Créer un profil d'activation pour enregistrer des terminaux non gérés avec BlackBerry 2FA

Procédez comme suit pour créer un profil d'activation pour les utilisateurs de terminaux non gérés par BlackBerry UEM. Ces terminaux doivent être enregistrés via BlackBerry UEM pour pouvoir être utilisés avec BlackBerry 2FA. Ce type d'activation s'applique uniquement aux terminaux iOS et Android.

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Stratégies et profils** dans la barre de menus.
2. Cliquez sur + en regard d'**Activation**.
3. Saisissez le nom et la description du profil.
4. Dans le champ **Nombre de terminaux qu'un utilisateur peut activer**, spécifiez le nombre maximum de terminaux que l'utilisateur peut activer.
5. Dans la liste déroulante **Propriété du terminal**, effectuez l'une des actions suivantes :
   - Si certains utilisateurs activent des terminaux personnels et d'autres des terminaux professionnels, sélectionnez **Non spécifié**.
   - Si les utilisateurs activent généralement des terminaux professionnels, sélectionnez **Professionnel**.
   - Si les utilisateurs activent généralement des terminaux personnels, sélectionnez **Personnel**.

6. Vous pouvez, à votre convenance, sélectionner un avis d'entreprise dans la liste déroulante **Attribuer un avis d'entreprise**. Si vous attribuez un avis d'entreprise, les utilisateurs activant des terminaux iOS doivent accepter l'avis pour terminer l'activation.
7. Dans la section **Types de terminaux que les utilisateurs peuvent activer**, sélectionnez les types de terminaux iOS et Android.
8. Cliquez sur l'onglet du terminal **iOS** ou **Android** et procédez comme suit :
   - Dans la liste déroulante **Limites de modèles de terminaux**, sélectionnez si vous souhaitez autoriser uniquement les terminaux spécifiés ou n'appliquer aucune restriction. Si vous choisissez de n'appliquer **aucune restriction**, cliquez sur **Modifier**, sélectionnez les terminaux que vous souhaitez interdire ou autoriser, puis cliquez sur **Enregistrer.**
   - Dans la liste déroulante **Version autorisée**, sélectionnez la version minimale autorisée.
   - Dans la section **Type d'activation**, sélectionnez **Enregistrement de terminaux pour BlackBerry 2FA uniquement**.
9. Cliquez sur **Ajouter**.

Attribuer un profil d'activation d'enregistrement uniquement à un utilisateur disposant d'un terminal non géré

Procédez comme suit pour attribuer un profil d'activation aux utilisateurs de terminaux non gérés par BlackBerry UEM. Ces terminaux doivent être enregistrés via BlackBerry UEM pour pouvoir être utilisés avec BlackBerry 2FA. Ce type d'activation est disponible uniquement pour les terminaux iOS et Android.

Avant de commencer :

- Créer un profil d'activation pour enregistrer des terminaux non gérés avec BlackBerry 2FA.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Utilisateurs** sur la barre de menu.
2. Recherchez un utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom de l'utilisateur.
4. Dans la section **Stratégie informatique et profils**, cliquez sur +.
5. Cliquez sur **Activation**.
6. Dans la liste déroulante **Profil d'activation**, cliquez sur le profil d'activation que vous avez créé pour autoriser l'enregistrement de terminaux non gérés utilisés avec BlackBerry 2FA.
7. Si le profil que vous avez sélectionné à l'étape 6 est déjà directement attribué à l'utilisateur, cliquez sur **Remplacer**. Sinon, cliquez sur **Attribuer**.

Activer un terminal BlackBerry 10

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

1. Sur le terminal, naviguez jusqu'à **Paramètres**.
2. Appuyez sur **Comptes**.
3. Si vous disposez de comptes existants sur ce terminal, appuyez sur **Ajouter un compte**. Sinon, passez à l'étape 4.
4. Appuyez sur **Messagerie, calendrier et contacts**.
5. Saisissez votre adresse électronique professionnelle et appuyez sur **Suivant**.
6. Dans le champ **Mot de passe**, saisissez le mot de passe d'activation que vous avez reçu. Appuyez sur **Suivant**.

7. Si vous recevez un avertissement vous indiquant que votre terminal n'a pas pu rechercher les informations de connexion, procédez comme suit :
   a) Appuyez sur **Avancé**.
   b) Appuyez sur **Compte professionnel**.
   c) Dans le champ **Adresse du serveur**, saisissez l'adresse du serveur. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
   d) Sélectionnez **Terminé**.
8. Suivez les instructions à l'écran pour terminer le processus d'activation.

À la fin : Pour vérifier que le processus d'activation a réussi, effectuez l'une des actions suivantes :

- Sur le terminal, accédez à BlackBerry Hub et vérifiez que l'adresse électronique est présente. Accédez au Calendrier et vérifiez que les rendez-vous sont présents.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.
- Vérifiez que l'application BlackBerry 2FA a été automatiquement téléchargée et installée sur le terminal de l'utilisateur en vérifiant son espace Travail. Si ce n'est pas le cas, l'application BlackBerry 2FA peut être téléchargée depuis BlackBerry World pour le travail.

Activer un terminal iOS

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

1. Installez BlackBerry UEM Client sur le terminal. Vous pouvez le télécharger depuis Apple App Store.
2. Sur le terminal, sélectionnez **BlackBerry UEM**.
3. Lisez l'accord de licence et sélectionnez **J'accepte**.
4. Saisissez votre adresse électronique professionnelle et sélectionnez **Go**.
5. Si nécessaire, saisissez l'adresse du serveur, puis sélectionnez **Go**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
6. Vérifiez que les détails du certificat affichés sur le terminal sont corrects et sélectionnez **Accepter**. Si votre administrateur vous a envoyé les détails du certificat séparément, vous pouvez comparer les informations affichées avec celles que vous avez reçues.
7. Saisissez votre mot de passe d'activation et sélectionnez **Activer mon terminal**.
8. Sélectionnez **OK** pour installer le certificat requis.
9. Suivez les instructions à l'écran pour procéder à l'installation.
10. Si vous êtes invité à saisir le mot de passe de votre compte de messagerie ou le mot de passe de votre terminal, suivez les instructions à l'écran.

À la fin : Pour vérifier que le processus d'activation a réussi, effectuez l'une des actions suivantes :

- Sur le terminal, ouvrez BlackBerry UEM Client et sélectionnez **À propos de**. Dans les sections **Terminal activé** et **État de conformité**, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

Activer un terminal Android

Envoyez les instructions d'activation suivantes à l'utilisateur du terminal.

1. Installez BlackBerry UEM Client sur le terminal. Vous pouvez télécharger BlackBerry UEM Client depuis Google Play.
2. Sur le terminal, sélectionnez **BlackBerry UEM**.
3. Lisez l'accord de licence et sélectionnez **J'accepte**.
4. Saisissez votre adresse électronique professionnelle et appuyez sur **Suivant**.
5. Si nécessaire, saisissez l'adresse du serveur, puis sélectionnez **Suivant**. Vous trouverez l'adresse du serveur dans l'e-mail d'activation que vous avez reçu ou dans BlackBerry UEM Self-Service.
6. Vérifiez que les détails du certificat affichés sur le terminal sont corrects et sélectionnez **Accepter**. Si votre administrateur vous a envoyé les détails du certificat séparément, vous pouvez comparer les informations affichées avec celles que vous avez reçues.
7. Saisissez votre mot de passe d'activation et sélectionnez **Activer mon terminal**.
8. Appuyez sur **Suivant**.
9. Appuyez sur **Activer**.

À la fin : Pour vérifier que le processus d'activation a réussi, effectuez l'une des actions suivantes :

- Sur le terminal, ouvrez BlackBerry UEM Client et sélectionnez **À propos de**. Dans la section **Terminal activé**, assurez-vous de la présence des informations sur le terminal et de l'heure et de la date d'activation.
- Dans BlackBerry UEM Self-Service, vérifiez que votre terminal est répertorié en tant que terminal activé. Le statut peut prendre jusqu'à deux minutes pour se mettre à jour après que vous avez activé le terminal.

Configurer ou annuler la pré-authentification

Effectuez la tâche suivante si votre entreprise contrôle la pré-authentification BlackBerry 2FA par l'intermédiaire de demandes d'assistance informatique ou si vous voulez remplacer les paramètres de pré-authentification actuels d'un utilisateur.

Avant de commencer :

- Vérifiez qu'un profil BlackBerry 2FA est attribué à l'utilisateur.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Utilisateurs** sur la barre de menu.
2. Recherchez un utilisateur.
3. Dans les résultats de la recherche, cliquez sur le nom de l'utilisateur.
4. Dans le résumé de l'utilisateur, cliquez sur **Activer le contournement pour BlackBerry 2FA**
5. Dans la boîte de dialogue **Configurer la période de contournement** spécifiez la durée (en heures) pendant laquelle l'utilisateur peut accéder aux ressources de votre entreprise sans devoir répondre à une demande de confirmation sur son terminal ou à envoyer un mot de passe à usage unique à partir d'un jeton.
6. Cliquez sur **Enregistrer**. La durée s'affiche dans l'écran d'informations sur l'utilisateur.
7. Vous pouvez également cliquer sur **Annuler** dans l'écran d'informations sur l'utilisateur pour mettre fin à la période de pré-authentification. Les utilisateurs peuvent également mettre fin à la période de pré-authentification en cliquant sur **Expire maintenant** dans BlackBerry UEM Self-Service.

Étapes à suivre pour gérer les jetons matériels de mot de passe à usage unique

Pour utiliser la fonctionnalité de jetons de mot de passe à usage unique (OTP), vous devez procéder comme suit :

Étape	Action
1	Activer la fonctionnalité de jetons OTP.
2	Si nécessaire, pour convertir un fichier d'informations de jeton .xml au format PSKC en fichier .csv, vous pouvez l'importer vers BlackBerry UEM, Utilisez l'outil de conversion de jeton BlackBerry 2FA. Pour plus d'informations, reportez-vous à Modification du fichier de configuration CSVConfig.
3	Importer des jetons OTP dans BlackBerry UEM
4	Attribuer un jeton OTP à un utilisateur

Activer la fonctionnalité de jetons OTP

1. Dans la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Jetons de mot de passe à usage unique**.
2. Cliquez sur **Activer**.
3. Cliquez sur **Activer**.

Désactiver la fonctionnalité de jetons OTP

1. Dans la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Jetons de mot de passe à usage unique**.
2. Cliquez sur **Désactiver la gestion de jetons de mot de passe à usage unique**.
3. Le cas échéant, supprimez les jetons OTP de BlackBerry UEM. Pour plus d'informations, reportez-vous à Supprimer un jeton OTP de BlackBerry UEM.

Jetons matériels de mot de passe à usage unique pris en charge

BlackBerry 2FA prend actuellement en charge les jetons matériels de mot de passe à usage unique (OTP) tiers suivants :

- RCDevs RC200
- Vasco DIGIPASS GO 6

- Feitian OTP C200

Davantage de jetons matériels pris en charge seront inclus dans les prochaines versions. Pour obtenir les dernières informations sur la compatibilité des jetons matériels, reportez-vous à la matrice de compatibilité du serveur.

Utilisez l'outil de conversion de jeton BlackBerry 2FA

Remarque : Cet outil est uniquement disponible et requis pour BlackBerry UEM 12.7. Pour les versions 12.8 et ultérieures de BlackBerry UEM et BlackBerry UEM Cloud, les fichiers d'information des jetons peuvent être importés directement dans UEM sans utiliser l'outil.

Utilisez l'outil de conversion de jeton BlackBerry 2FA pour convertir un fichier d'informations de jeton .xml au format PSKC en fichier .csv que vous pouvez importer dans BlackBerry UEM. Une fois le fichier converti, le fichier généré est automatiquement enregistré dans le même dossier que l'outil.

Pour les jetons Vasco et Feitian, vous devez utiliser l'outil de conversion de jeton BlackBerry 2FA afin de convertir les fichiers d'informations de jeton que le fabricant de jetons fournit dans un format lisible par BlackBerry UEM.

L'outil de conversion de jeton BlackBerry 2FA prend uniquement en charge les fichiers d'informations de jeton au format PSKC. Pour plus d'informations sur PSKC, reportez-vous à https://tools.ietf.org/html/rfc6030.

Important : Le fichier généré contient des informations de jeton dans un format non crypté. Il est fortement recommandé d'exécuter l'outil de conversion de jeton BlackBerry 2FA uniquement dans un environnement informatique sécurisé et de supprimer le fichier généré immédiatement après son importation dans BlackBerry UEM.

Avant de commencer :

- Téléchargez l'outil de conversion de jeton BlackBerry 2FA à l'adresse https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B.
- Placez les fichiers d'informations de jeton que vous voulez convertir dans le même dossier que l'outil.

1. Ouvrez la ligne de commande.
2. Accédez au répertoire de l'outil de conversion de jeton BlackBerry 2FA.
3. Exécutez **tokenConversionTool-**<*version*>**.jar** avec les paramètres suivants :

Paramètre	Description
-h	Permet d'afficher le message d'utilisation de l'aide.
-v	Permet d'activer le mode verbose (facultatif). Si vous activez le mode verbose, les informations de jeton dans le fichier spécifié sont affichées dans la ligne de commande.
-f	Vous pouvez éventuellement indiquer le format dans lequel vous souhaitez réaliser la conversion ('basic' ou 'rcdevs'). La valeur par défaut est 'rcdevs'.
-p	Si nécessaire, spécifiez la clé de jeton qui est obligatoire pour déchiffrer le fichier d'informations de jeton. Le mot de passe est une séquence d'octets au format hexadécimal (par exemple, A12BC34D).

Paramètre	Description
filename	Indiquez le fichier que vous voulez convertir. Le fichier doit se trouver dans le même dossier que l'outil. Ce paramètre est obligatoire.

Par exemple, saisissez l'un des éléments suivants :

- `java -jar <toolName>.jar -f basic -p <password> ./<tokenFileName>.xml`
- `java -jar tokenConversionTool-1.0.4.jar ./vasco.xml`

Le chemin du fichier de sortie apparaît lorsque le fichier est généré.

À la fin : Importez le fichier d'informations de jeton généré dans la console de gestion BlackBerry UEM. Pour plus d'informations, reportez-vous à Importer des jetons OTP dans BlackBerry UEM.

Modification du fichier de configuration CSVConfig

Le fichier .csv contenant les données de jetons nécessite un fichier de configuration (CSVConfig.json) qui définit la manière dont BlackBerry UEM analyse le fichier .csv. Le fichier .csv doit être analysé correctement avant que les données de jetons soient extraites et importées dans la base de données BlackBerry UEM.

Lors de votre première connexion à BlackBerry UEM après avoir activé la fonctionnalité de jetons OTP, un fichier CSVConfig.json par défaut est généré. Le fichier est généré avec des valeurs par défaut et enregistré dans "BESNG_HOME"/otp/config/CSVConfig.json (ou C:\otp\config\CSVConfig.json).

Les informations suivantes vous aideront à modifier votre fichier CSVConfig.json pour vous assurer que BlackBerry UEM analyse votre fichier .csv correctement.

- Le paramètre d'extension recommandé est « CSV ».
- Le paramètre recommandé pour « stripSpacesAndQuotations » est « true ». Tous les espaces et les guillemets des colonnes sont supprimés.
- Les colonnes de chaque champ de données peuvent comporter un maximum de quatre paramètres permettant de déterminer comment BlackBerry UEM analyse et extrait les données de la colonne correspondante.
  - « column » détermine le numéro de colonne dans le fichier .csv. Les colonnes commencent à « 0 ».
  - « startCharPos » détermine où débutent les données de jetons dans la colonne. Si « stripSpacesAndQuotations » est défini sur « true », seuls les caractères situés avant le début des données de jetons sont comptés, sans tenir compte des espaces et des guillemets.
  - « endCharPos » détermine où se terminent les données des jetons dans les colonnes. Si « stripSpacesAndQuotations » est défini sur « true », seuls les caractères situés avant la fin des données de jetons sont comptés, sans tenir compte des espaces et des guillemets.
  - « encoding » détermine le codage/décodage de caractères utilisé. « base64 » est la norme.

L'exemple ci-dessous présente un fichier CSVConfig.json mis à jour aux fins d'analyser un fichier .csv rempli d'informations sur les jetons RCDevs :

```
{
   "extension" : "CSV",
   "stripSpacesAndQuotations" : true,
   "startRow" : 4,
   "token_serial_number" : {
      "column" : 1,
      "startCharPos" : 0
```

```
   },
   "password_seed" : {
      "column" : 3,
      "startCharPos" : 9,
      "encoding" : "base64"
   },
   "password_length" : {
      "column" : 6,
      "startCharPos" : 10,
      "encoding" : "base64"
   },
   "time_step" : {
      "column" : 7,
      "startCharPos" : 13,
      "encoding" : "base64"
   },
   "vendor" : {
      "column" : 2,
      "startCharPos" : 0,
      "endCharPos" : 6
   },
   "model" : {
      "column" : 2,
      "startCharPos" : 6,
      "endCharPos" : 14
   },
   "t0" : {
      "column" : 5,
      "startCharPos" : 11,
      "encoding" : "base64"
   }
}
```

L'exemple ci-dessous présente un texte brut d'un fichier .csv rempli d'informations sur les jetons RCDevs :

```
1 # Inventory Import File for RCDevs WebADM
2 # Generated on June 29, 2016, 2:40 pm
3
4 Type               Reference             Description                  Data
5 "OTP Token", "2308602200271", "RCDevs RC200-T6",
 "TokenKey=P6chCRszGaawHhpzWUHCS8Ua8WE=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
6 "OTP Token", "2308602200272", "RCDevs RC200-T6",
 "TokenKey=Zghe8fbekGOXpwGM2vmEcZyZnaE=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
7 "OTP Token", "2308602200273", "RCDevs RC200-T6",
 "TokenKey=EH//86f6pnup3F4AS7w7HNazYjU=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
8 "OTP Token", "2308602200274", "RCDevs RC200-T6", "TokenKey=tzrVqKFMns9/
rbAyCYCdDxb04Ig=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
9 "OTP Token", "2308602200275", "RCDevs RC200-T6", "TokenKey=0FuZ/
A6ZCVGClaYW3EFCtXWNFFk=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
```

Importer des jetons OTP dans BlackBerry UEM

Pour importer des jetons OTP, vous avez besoin d'un fichier .csv (séparé par des virgules) qui contient les informations sur les jetons. Le fichier.csv est lu par BlackBerry UEM à l'aide d'un fichier de configuration (CSVConfig.json).

Avant de commencer : Vous devez modifier le fichier par défaut CSVConfig.json de telle manière que BlackBerry UEM puisse analyser puis stocker les informations des jetons dans la base de données. Pour plus d'informations, reportez-vous à Modification du fichier de configuration CSVConfig.

1. Dans la barre de menu, cliquez sur **Paramètres** > **Intégration externe** > **Jetons de mot de passe à usage unique**.
2. Cliquez sur **Parcourir**.
3. Accédez au fichier .csv qui contient les informations sur les jetons et sélectionnez-le.
4. Cliquez sur **Télécharger**.

Supprimer un jeton OTP de BlackBerry UEM

1. Dans la barre de menu, cliquez sur **Paramètres** > **Intégration externe** > **Jetons de mot de passe à usage unique**.
2. Recherchez le numéro de série du jeton que vous souhaitez supprimer et sélectionnez-le.
3. Cliquez sur  .
4. Cliquez sur **Supprimer**.

Attribuer un jeton OTP à un utilisateur

Avant de commencer : Attribuer un profil BlackBerry 2FA à un utilisateur.

1. Sur la barre de menus, cliquez sur **Utilisateurs**. Recherchez le nom de l'utilisateur et sélectionnez-le.
2. Sur la page d'informations de l'utilisateur, cliquez sur **Jetons de mot de passe à usage unique**.
3. Recherchez le numéro de série du jeton que vous souhaitez attribuer à l'utilisateur et sélectionnez-le.
4. Cliquez sur **Attribuer**.

Supprimer un jeton OTP d'un utilisateur

1. Sur la barre de menus, cliquez sur **Utilisateurs**. Recherchez le nom de l'utilisateur et sélectionnez-le.
2. Sur la page d'informations de l'utilisateur, cliquez sur **Jetons de mot de passe à usage unique**.
3. Sous **Jetons attribués**, cliquez sur **Supprimer** .
4. Cliquez sur **Envoyer** pour annuler l'attribution du jeton de mot de passe à usage unique.

Prise en charge automatique des jetons matériels désynchronisés

Vous pouvez régler le saut de temps pour que les jetons matériels prennent automatiquement en charge la dérive de jeton. Quand l'horloge interne d'un jeton matériel dérive trop loin de l'heure exacte, le jeton affiche des codes non valides. Si vous augmentez le saut de temps, le code de cette fenêtre est valide, même si le jeton n'est pas synchronisé.

Par exemple, si vous réglez le saut temps sur « 2 », le code qui s'affiche sur le jeton est accepté comme un code valide s'il précède ou suit le code attendu de deux intervalles d'actualisation. Dans cet exemple, si le code affiché sur le jeton est le troisième code précédant ou suivant le code attendu, le code est considéré comme non valide et le mot de passe à usage unique est rejeté.

Ce paramètre règle le saut de temps pour tous les jetons matériels. Réglez le saut de temps en fonction du nombre d'intervalles d'actualisation qui vous font penser que les jetons ne sont pas synchronisés.

1. Dans la console de gestion, cliquez sur **Paramètres > Intégration externe**.
2. Cliquez sur **Jetons de mot de passe à usage unique BlackBerry 2FA**.
3. Dans le champ **Fenêtre de pas de temps**, cliquez sur  .
4. Saisissez une valeur comprise entre 0 et 50. La valeur par défaut est 3. Pour accepter uniquement le code attendu, qui peut correspondre ou ne pas correspondre au code affiché sur le jeton, définissez la valeur du saut de temps sur 0.
5. Cliquez sur **Mettre à jour**.

Resynchronisation manuelle d'un jeton matériel

Si un jeton matériel de mot de passe à usage unique attribué à un utilisateur devient inutilisable parce que la dérive n'a pas été prise en charge automatiquement, vous pouvez essayer de resynchroniser manuellement le jeton. Pour resynchroniser manuellement un jeton à l'aide de BlackBerry UEM, l'utilisateur doit vous donner deux nouveaux codes consécutifs.

1. Sur la barre de menus, cliquez sur **Utilisateurs**. Recherchez le nom de l'utilisateur et sélectionnez-le.
2. Cliquez sur **Jetons de mot de passe à usage unique**.
3. Dans la section **Jeton attribué**, cliquez sur **Resynchroniser**.
4. Dans le champ **Saut de temps**, saisissez le nombre maximum de sauts de temps que vous voulez resynchroniser sur le jeton désynchronisé.
5. Dans le champ **Premier code de jeton**, saisissez le code qui s'affiche sur le jeton.
6. Dans le champ **Deuxième code de jeton**, saisissez le code consécutif suivant qui s'affiche sur le jeton.
7. Cliquez sur **Resynchroniser**.

Journalisation et rapports

BlackBerry UEM crée des journaux pour les fonctionnalités de pré-authentification et de résolution autonome de BlackBerry 2FA. Les journaux sont stockés dans le fichier journal BlackBerry UEM Core (CORE).

Outre la journalisation d'informations à des fins de résolution de problèmes généraux, BlackBerry UEM crée des lignes de journaux spéciales pour les activités de pré-authentification et de résolution autonome à des fins d'audit. Vous pouvez extraire ces lignes de fichiers journaux pour contrôler l'utilisation globale des fonctionnalités de pré-authentification et de résolution autonome. Ces lignes de journaux sont consignées au niveau INFO et se composent de données séparées par des virgules, préfixées par des informations de journaux CORE universelles qui peuvent être annulées.

Ces lignes de journaux spéciales sont marquées par des marqueurs qui vous permettent de les extraire facilement. Deux types d'activités sont contrôlés : les demandes de pré-authentification et les demandes d'authentification au cours de la pré-authentification de l'utilisateur. Lors de l'extraction de ces lignes et de l'annulation des informations de journaux CORE universelles, vous pouvez ouvrir les données séparées par des virgules dans n'importe quel logiciel prenant en charge le format CSV. Pour plus d'informations sur la journalisation et la création de rapports, reportez-vous au contenu relatif à la maintenance et la surveillance de BlackBerry UEM.

Audit des demandes de pré-authentification

BlackBerry UEM journalise chaque demande de pré-authentification BlackBerry 2FA et chaque demande d'authentification au cours de la pré-authentification. Les données sont journalisées lorsque la demande se termine ou expire.

Le fichier journal d'audit comprend les informations suivantes sur chaque demande de pré-authentification :

- Marqueur 1 : BB2FA_AUDIT. Il s'agit de l'identificateur de toutes les lignes de journaux d'audit BlackBerry 2FA du journal BlackBerry UEM Core. Il indique également où couper les lignes de journaux pour annuler les informations du journal CORE universel.
- Marqueur 2 : PREAUTH_REQUEST. Il s'agit de l'identificateur du type d'évènement (demande de pré-authentification).
- Date
- Heure
- Source : console de gestion BlackBerry UEM, terminal de l'utilisateur BlackBerry UEM Self-Service
- Nom d'utilisateur
- Nom du profil BlackBerry 2FA : le nom est journalisé entre guillemets pour éviter que le champ soit divisé par des virgules dans le profil.
- Durée de pré-authentification demandée en heures
- Durée de pré-authentification maximale configurée en heures
- Résultat : SUCCESS, FAILED_INVALID_REQUEST
- Heure d'expiration de la pré-authentification

Par exemple :

```
2BB2FA_AUDIT,PREAUTH_REQUEST,2016-11-05,13:27:17.822,admin,user1,"Sales BB2FA
 Profile",3,12,May 11 16:41
```

Le fichier journal d'audit comprend les informations suivantes sur chaque demande d'authentification au cours de la pré-authentification :

- Marqueur 1 : BB2FA_AUDIT. Il s’agit de l’identificateur de toutes les lignes de journaux d’audit BlackBerry 2FA du journal BlackBerry UEM Core. Il indique également où couper les lignes de journaux pour annuler les informations du journal CORE universel.
- Marqueur 2 : AUTH_USER_IN_PREAUTH. Il s'agit de l'identificateur du type d'événement (demande d'authentification au cours de la pré-authentification).
- Date
- Heure
- ID de transaction
- Source : application BlackBerry 2FA, BlackBerry Enterprise Identity, etc.
- Nom d'utilisateur
- Stratégie d'authentification : mot de passe d'entreprise, mot de passe de terminal actif, mot de passe de terminal passif
- Nom du profil : le nom est journalisé entre guillemets pour éviter que le champ soit divisé par des virgules dans le profil..
- Heure d'expiration de la pré-authentification

Par exemple :

```
BB2FA_AUDIT,AUTH_USER_IN_PREAUTH,2016-11-05,13:27:17.822,50dbe1cc,BB2FA,user1,Enterprise
 Password,"Sales BB2FA Profile",May 11 16:41
```

Informations juridiques

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, DEMANDE OU ACTION ENTREPRISE PAR VOUS, NOTAMMENT POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUT 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 AYANT-DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES DE TEMPS DE COMMUNICATION), 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, DISTRIBUTEURS, FOURNISSEURS, SOUS-TRAITANTS INDÉPENDANTS 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 sans fil prend en charge toutes les fonctionnalités. Certains fournisseurs de services sans fil 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 ni garanties expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers. 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
2 200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
Royaume-Uni

Publié au Canada