



BlackBerry 2FA

Présentation

Table des matières

- À propos de BlackBerry 2FA..... 4**
- Authentification directe.....5**
- Jetons OTP..... 6**
- Pré-authentification et résolution autonome..... 7**
- Architecture : BlackBerry 2FA..... 8**
 - Demands d'authentification via BlackBerry UEM.....9
 - Réponses d'authentification via BlackBerry UEM..... 11
 - Demands d'authentification via BlackBerry UEM Cloud..... 12
 - Réponses d'authentification via BlackBerry UEM Cloud..... 13
- Informations juridiques..... 14**

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 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 2FA pour protéger une large gamme de systèmes, parmi lesquels des VPN, des systèmes compatibles RADIUS, des applications personnalisées qui utilisent une API REST et des services en nuage 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 de mot de passe à usage unique (OTP) basés sur des normes sont enregistrés dans la console BlackBerry UEM et émis 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 [Guide d'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 en nuage et les autres systèmes pris en charge. Pour plus d'informations, reportez-vous au [contenu relatif à la matrice 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 Application ou Contenu de BlackBerry Enterprise Mobility Suite, ou des licences utilisateur 2FA distinctes. Pour l'édition Collaboration, BlackBerry 2FA peut être utilisé pour s'authentifier auprès des applications BlackBerry et de Microsoft Office 365 uniquement. Pour plus d'informations sur BlackBerry 2FA, y compris sur le mode d'achat de 2FA, consultez les informations sur blackberry.com.

Authentification directe

Vous pouvez activer la fonctionnalité d'authentification directe afin que les utilisateurs, lorsqu'ils souhaitent s'authentifier auprès des ressources de votre organisation, commencent le processus d'authentification à partir de leurs terminaux et non pas avec une invite de confirmation, et sans utiliser de mot de passe à usage unique. Lorsque vous activez la fonctionnalité d'authentification directe pour les utilisateurs, ceux-ci doivent utiliser leur mot de passe de répertoire pour se connecter aux ressources de votre organisation dans le délai que vous indiquez.

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

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](#).

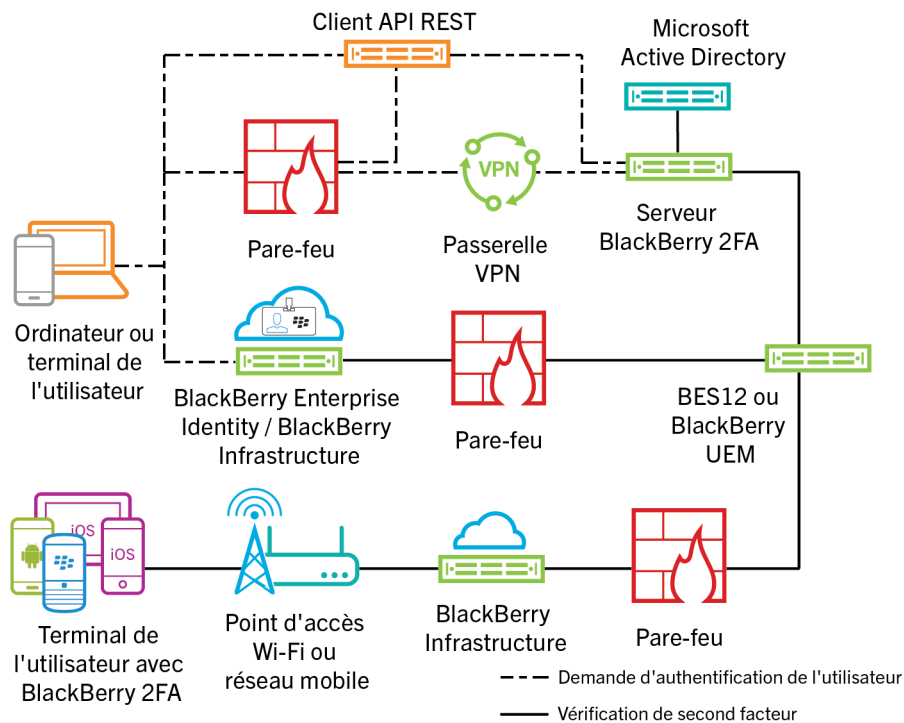
Pré-authentification et résolution autonome

La pré-authentification et la résolution autonome sont des fonctionnalités de BlackBerry 2FA qui permettent aux utilisateurs de s'authentifier aux ressources de votre organisation 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.

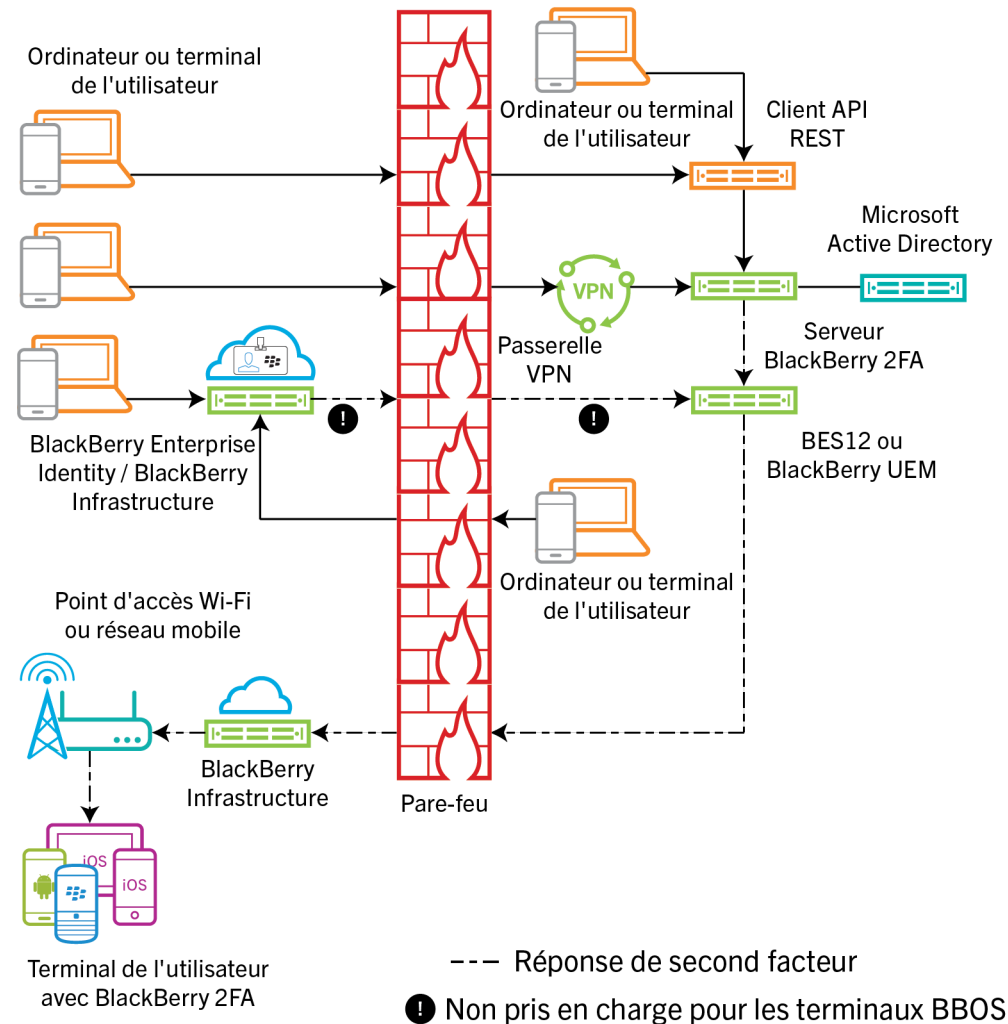
Architecture : BlackBerry 2FA



| 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. |

| Composant | Description |
|---|---|
| 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. |
| 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



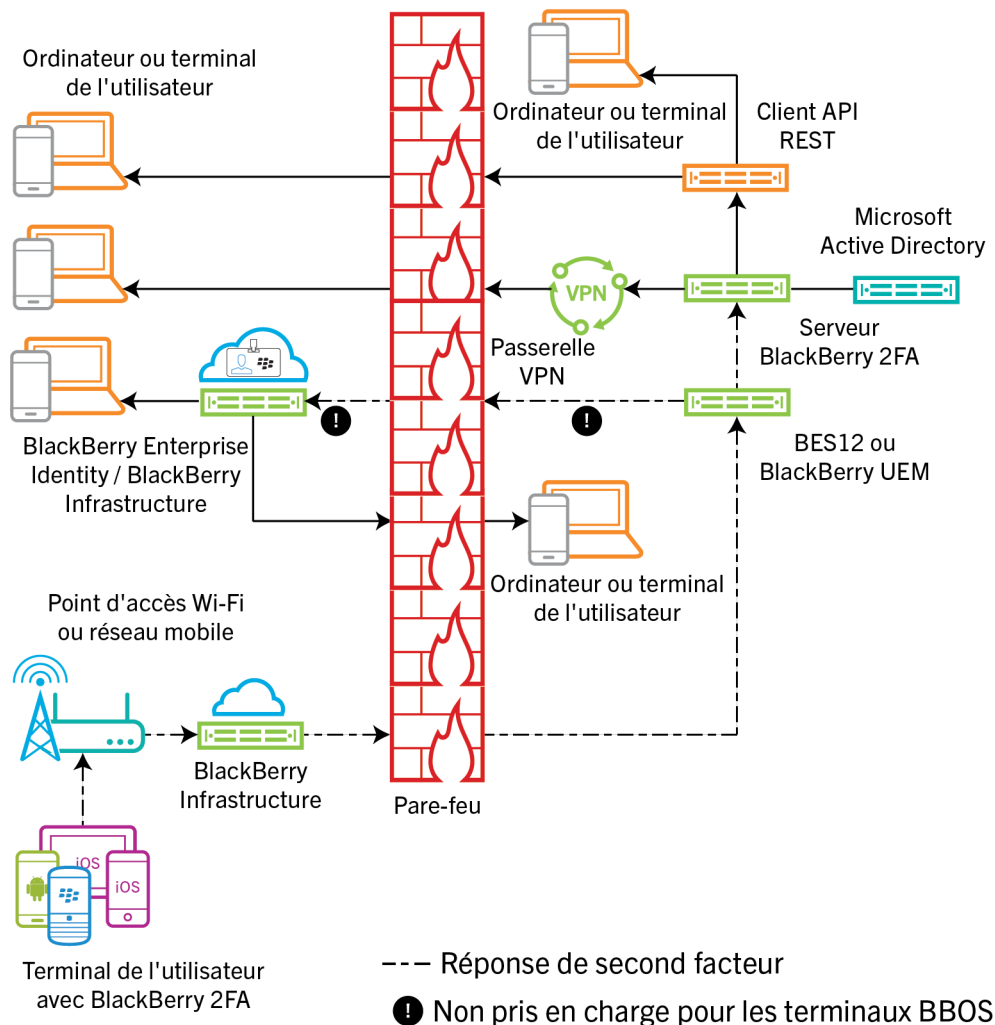
Pour initier une demande d'authentification, un utilisateur doit effectuer l'une des opérations suivantes :

- 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 reconnaître 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).

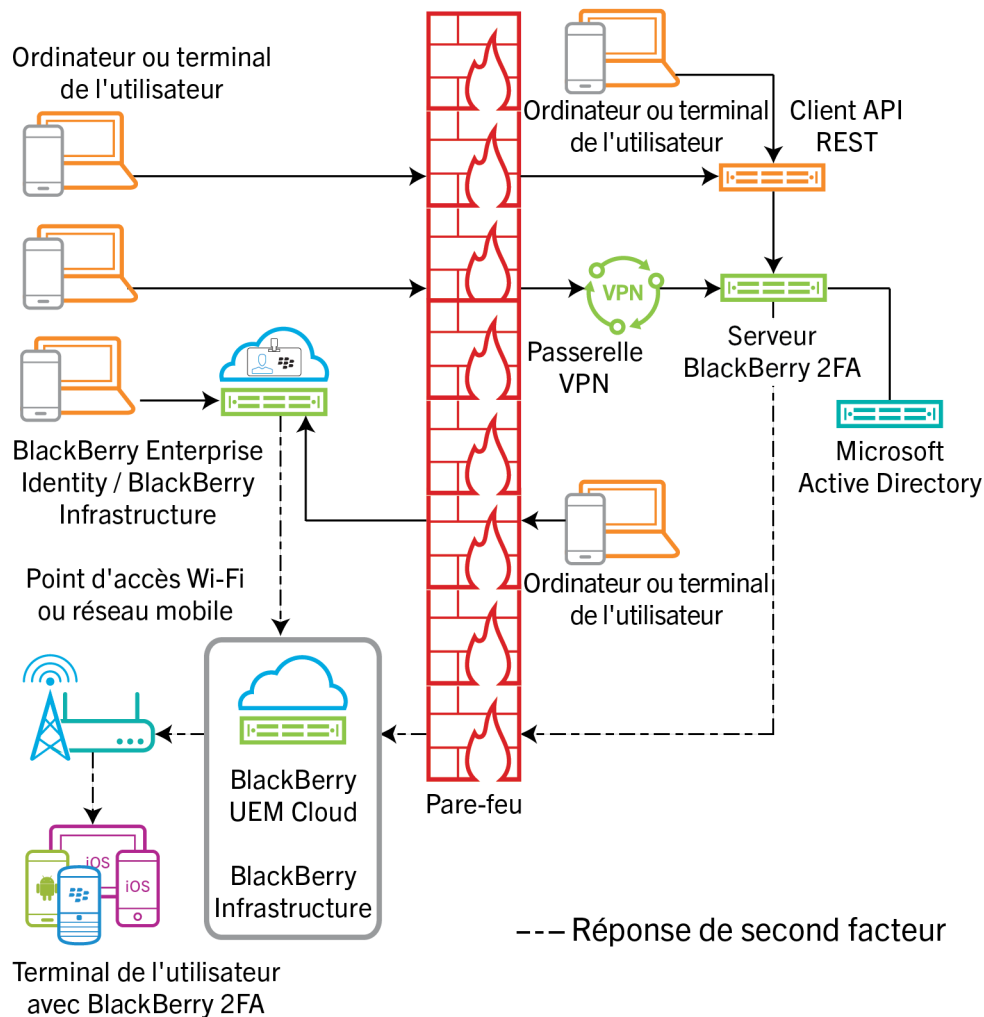
Réponses d'authentification via BlackBerry UEM



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'authentications qui utilisent des jetons de mot de passe à usage unique (OTP).

Demandes d'authentification via BlackBerry UEM Cloud



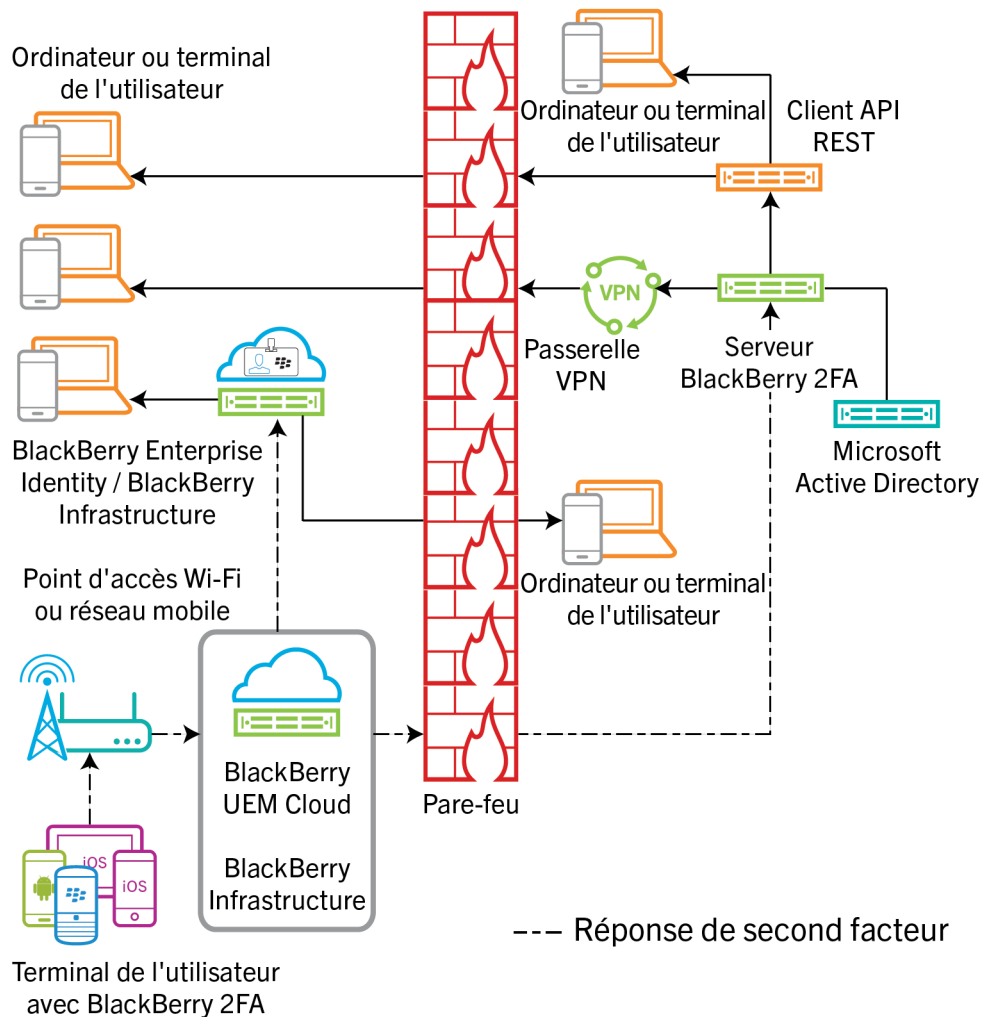
Pour initier une demande d'authentification, un utilisateur doit effectuer l'une des opérations suivantes :

- 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 reconnaître 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).

Informations juridiques

©2018 BlackBerry Limited. Les marques commerciales, notamment BLACKBERRY, BBM, BES et son emblème, ATHOC, MOVIRTU 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 marques commerciales sont expressément réservés. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

Android est une marque commerciale de Google Inc. iOS est une marque commerciale de Cisco Systems, Inc. et/ou ses filiales aux États-Unis. et dans certains autres pays. iOS® est utilisé sous licence par Apple Inc. Microsoft et Windows sont des marques commerciales ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. 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 secrets commerciaux et/ou des informations confidentielles et propriétaires 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 D'UN LOGICIEL, MATÉRIEL, 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 LA GARANTIE LIMITÉE APPLICABLE, L'ACCORD DE LICENCE DU LOGICIEL BLACKBERRY ET/OU 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 L'UTILISATION OU NON-UTILISATION DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT 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 COÛTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COÛT DE BIENS DE SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COÛTS 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), REVENEURS 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