BlackBerry 2FA

Guide de configuration du serveur

3.4

Table des matières

Procédure de configuration du serveur BlackBerry 2FA

Pour configurer le serveur BlackBerry 2FA, procédez comme suit .

Tâche	Description
1	Si nécessaire, téléchargez et installez le serveur BlackBerry 2FA. Après avoir installé le serveur, vous devez générer et télécharger un fichier d'activation et l'utiliser pour activer la communication entre le serveur BlackBerry 2FA et BlackBerry UEM. Pour plus d'informations, consultez le contenu relatif à l'installation et à la mise à niveau de BlackBerry 2FA.
2	Sur le serveur VPN, créez un profil pour le serveur BlackBerry 2FA. Pour plus d'informations, reportez-vous à Configuration d'une connexion entre le serveur BlackBerry 2FA et une passerelle VPN.
3	Configuration du serveur BlackBerry 2FA pour se connecter à une passerelle VPN
4	Configuration de la connexion au point de terminaison d'API REST
5	Création d'un client d'API REST dans le serveur BlackBerry 2FA
6	Autorisation de l'authentification MS-CHAP pour les utilisateurs d'un domaine
7	Configuration de l'application BlackBerry 2FA
8	Attribution d'une configuration d'une passerelle VPN ou d'un client REST à un groupe d'utilisateurs
9	Si nécessaire, envoyez l'application BlackBerry 2FA aux terminaux. Pour plus d'informations, reportez-vous à Installez l'application BlackBerry 2FA sur les terminaux.

Configuration d'une connexion entre le serveur BlackBerry 2FA et une passerelle VPN

Sur votre serveur VPN, le serveur BlackBerry 2FA doit être configuré comme serveur RADIUS auquel les demandes d'authentification sont transférées. Le serveur BlackBerry 2FA effectue les tâches suivantes pour authentifier les utilisateurs afin qu'ils puissent se connecter à une passerelle VPN :

- Authentifie le terminal de l'utilisateur ou le mot de passe à usage unique (OTP)
- Agit comme proxy pour l'authentification de mot de passe
- Combine les deux résultats pour déterminer si l'authentification a réussi

Vous devez également configurer un profil client VPN ou un client qui permet aux utilisateurs de sélectionner BlackBerry 2FA lorsqu'ils se connectent au VPN à partir de leur ordinateur.

Pour chaque serveur BlackBerry 2FA de votre environnement, le serveur RADIUS doit avoir les options suivantes :

- Adresse IP ou élément FQDN de l'ordinateur qui héberge le serveur BlackBerry 2FA
- Délai compris entre 60 et 90 secondes pour la connexion entre le serveur VPN et le serveur BlackBerry 2FA
- Secret partagé unique
- Port d'authentification défini sur 1812
- En fonction des options d'authentification disponibles, l'une des options suivantes : PAP, MS-CHAP v1, MS-CHAP v2 ou EAP-MSCHAP

Le profil client VPN doit disposer d'un délai défini entre 30 et 60 secondes pour la connexion entre le client VPN sur l'ordinateur de l'utilisateur et le serveur VPN.

Pour obtenir des instructions sur la façon de configurer un serveur RADIUS ou un profil client VPN, consultez la documentation du serveur VPN que vous utilisez.

Pour obtenir la liste des serveurs VPN pris en charge, reportez-vous au contenu relatif à la matrice de compatibilité du serveur BlackBerry 2FA.

Protocoles d'authentification pris en charge pour chaque option d'authentification

Le tableau suivant présente les protocoles d'authentification disponibles pour chaque option d'authentification prise en charge par BlackBerry 2FA.

Remarque : Si vos utilisateurs utilisent des jetons de mot de passe à usage unique pour s'authentifier, le serveur VPN doit être configuré pour les authentifier à l'aide de PAP. Les OTP ne sont pas pris en charge par d'MSCHAPv1, MSCHAPv2 ou EAP-MSCHAP.

Option d'authentification	Protocoles d'authentification pris en charge
Authentification à deux facteurs à l'aide d'un mot de passe de terminal passif	PAP
Authentification à deux facteurs à l'aide d'un mot de passe de terminal actif	PAP
Authentification à deux facteurs à l'aide d'un mot de passe d'entreprise	MS-CHAP v1, MS-CHAP v2, PAP, EAP-MSCHAP

Option d'authentification	Protocoles d'authentification pris en charge
Authentification à facteur unique à l'aide d'un mot de passe d'entreprise	MS-CHAP v1, MS-CHAP v2, PAP, EAP-MSCHAP

Configuration de la connexion au serveur BlackBerry 2FA sur une passerelle VPN Cisco ASA Series

Si vous utilisez une passerelle VPN Cisco ASA Series, vous pouvez créer le profil VPN à l'aide des informations ci-dessous.

Pour obtenir des instructions détaillées sur la façon de configurer le profil VPN, consultez http://www.cisco.com pour lire la documentation Cisco ASA Series.

Lorsque vous créez le profil, vous devez définir les options suivantes pour prendre en charge BlackBerry 2FA :

- Pour chaque serveur BlackBerry 2FA de votre environnement, créez un groupe de serveurs RADIUS AAA avec les options suivantes :
  - Adresse IP ou élément FQDN de l'ordinateur qui héberge le serveur BlackBerry 2FA
  - Délai compris entre 60 et 90 secondes pour la connexion entre la passerelle VPN et le serveur BlackBerry 2FA
  - Secret partagé unique
  - Port d'authentification défini sur 1812
  - Élément MS-CHAP v2 compatible
- Pour la connexion entre le client VPN sur l'ordinateur de l'utilisateur et la passerelle VPN, définissez le délai entre 30 et 60 secondes. Vous devez configurer le délai dans le fichier de profil client VPN Cisco AnyConnect (un fichier XML) qui doit être installé sur l'ordinateur des utilisateurs.
- Option de gestion des mots de passe, si vous êtes en train de configurer le profil pour prendre en charge MS-CHAP v2

Vous devez effectuer les opérations suivantes pour terminer le processus de création de profil :

- Activer le protocole d'encapsulation de charge utile de tunnel VPN (par exemple, le protocole IPSEC-IKE v2)
- Toutes les commandes requises pour le groupe de stratégies VPN associé
- Toutes les commandes requises pour le profil client VPN Cisco AnyConnect associé et la création du fichier XML
- Toutes les commandes requises pour le groupe de tunnels VPN associé

Vous n'avez pas besoin de configurer une authentification de certificat supplémentaire.

Lorsque vous configurez la connectivité de passerelle VPN dans le serveur BlackBerry 2FA, vous devez fournir le secret partagé RADIUS que vous avez créé dans le profil VPN.

Configuration de la connexion au serveur BlackBerry 2FA sur Citrix NetScaler

Si vous utilisez Citrix NetScaler, vous pouvez configurer la connexion au serveur BlackBerry 2FA en l'ajoutant en tant que serveur RADIUS. Si vous avez plusieurs serveurs BlackBerry 2FA dans votre environnement, vous devez configurer un serveur RADIUS distinct pour chacun d'eux.

Pour obtenir des instructions détaillées sur la façon de configurer NetScaler pour se connecter au serveur BlackBerry 2FA, visitez la page http://docs.citrix.com/en-us/netscaler.html et consultez la section « Configuration de l'authentification RADIUS » dans la documentation système NetScaler.

Par exemple, vous pouvez configurer une connexion au serveur BlackBerry 2FA et utiliser BlackBerry 2FA comme méthode d'authentification par défaut. Si vous souhaitez configurer cet exemple, dans l'utilitaire de configuration pour NetScaler, vous devez définir les paramètres d'authentification sous les paramètres globaux comme suit :

- « Nombre maximal d'utilisateurs », « Nombre maximal de tentatives de connexion » et « Délai d'échec de connexion », tel que requis par votre organisation.
- Type d'authentification défini sur RADIUS
- Adresse IP définie sur le serveur BlackBerry 2FA
- Port défini sur 1812
- Délai compris entre 60 et 90 secondes pour la connexion entre NetScaler et le serveur BlackBerry 2FA
- Secret partagé unique
- Option « Activer l'extraction d'adresses IP NAS » sélectionnée
- Option « Encodage de mot de passe » définie sur le protocole d'authentification pris en charge par l'option d'authentification VPN que vous avez choisie (BlackBerry 2FA ne prend pas en charge l'option « chap »)
- Option Comptabilité désactivée

Configuration de la connexion au serveur BlackBerry 2FA sur F5 BIG-IP

Si vous utilisez F5 BIG-IP avec un serveur AAA, vous pouvez créer une stratégie d'accès avec Access Policy Manager à l'aide des informations ci-dessous.

Pour obtenir des instructions détaillées sur la façon de configurer l'authentification à l'aide de serveurs AAA, visitez https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm_config_10_2_0/apm_config_server_auth.html et consultez la documentation F5 BIG-IP.

Lorsque vous créez la stratégie, vous devez définir les options suivantes pour qu'elles prennent en charge BlackBerry 2FA :

- Définissez le type d'authentification sur RADIUS.
- Indiquez l'adresse IP ou l'élément FQDN de l'ordinateur qui héberge le serveur BlackBerry 2FA.
- Configurez un délai compris entre 60 et 90 secondes pour la connexion entre la passerelle VPN et le serveur BlackBerry 2FA.
- Définissez un secret partagé unique.
- Définissez le port d'authentification sur 1812.
- Vérifiez que MS-CHAP v2 est pris en charge.
- Désactivez la comptabilité.
- Indiquez le nombre maximal de tentatives de connexion.

La stratégie doit être attribuée à chaque serveur BlackBerry 2FA de votre environnement.

Configuration de la connexion au serveur BlackBerry 2FA sur un VPN SSL Barracuda

Si vous utilisez un VPN SSL Barracuda, vous pouvez configurer la connexion au serveur BlackBerry 2FA en l'ajoutant en tant que serveur RADIUS. Si vous avez plusieurs serveurs BlackBerry 2FA dans votre environnement, vous devez configurer un serveur RADIUS distinct pour chacun d'eux.

Pour obtenir des instructions détaillées sur la façon de configurer le VPN SSL Barracuda pour se connecter au serveur BlackBerry 2FA, consultez la page https://www.barracuda.com/support/knowledgebase/50160000000HZG9AAO.

Vous devez configurer un serveur RADIUS avec les options suivantes pour prendre en charge BlackBerry 2FA :

- Définissez le type d'authentification sur RADIUS.
- Indiquez l'adresse IP ou l'élément FQDN de l'ordinateur qui héberge le serveur BlackBerry 2FA.
- Configurez un délai compris entre 60 et 90 secondes pour la connexion entre la passerelle VPN et le serveur BlackBerry 2FA.
- Définissez un secret partagé unique.
- Définissez le port d'authentification sur 1812.
- Vérifiez que MS-CHAP v2 est pris en charge.
- Désactivez la comptabilité.
- Indiquez le nombre maximal de tentatives de connexion.

Configuration de la connexion au serveur BlackBerry 2FA sur un serveur strongSwan

Pour configurer la connectivité au serveur BlackBerry 2FA sur un serveur strongSwan, vous devez modifier les fichiers ipsec.conf et eap-radius.conf.

Pour plus d'informations sur ces fichiers et sur la façon de configurer strongSwan, visitez https://www.strongswan.org/.

Configuration du fichier ipsec.conf

Le fichier ipsec.conf se trouve dans le répertoire /etc. Vous devez ajouter une nouvelle section « conn » pour le serveur BlackBerry 2FA. Par exemple :

```
conn <name>
 keyexchange=ikev2
 rightauth=eap-radius
 rightsendcert=never
 eap_identity=%any
 auto=add
```

Paramètre	Description
<name>	Il s'agit du nom unique de la nouvelle section de connexion. En règle générale, ce nom reflète certaines caractéristiques clés de la connexion (par exemple, IPSec-IKEv2-radius).

Paramètre	Description
keyexchange=ikev2	Ce paramètre spécifie la méthode d'échange de clés (par exemple, IKEv1, IKEv2). Le serveur BlackBerry 2FA serveur n'utilise pas ce paramètre, mais vous devez l'inclure dans la section conn afin d'autoriser un échange de clés approprié avec les clients VPN. Vous devez vous assurer que les clients VPN qui se connectent au serveur strongSwan utilisent la même méthode d'échange de clés.
rightauth=eap-radius	Ce paramètre indique que le serveur strongSwan doit utiliser EAP sur RADIUS afin d'authentifier les clients VPN pour ce type de connexion.
rightsendcert=never	Ce paramètre indique que les certificats utilisateur ne sont pas utilisés pour l'authentification client.
eap_identity=%any	Ce paramètre indique l'identité du client VPN à utiliser pour l'authentification. Le serveur BlackBerry 2FA n'utilise pas ce paramètre, mais vous devez l'inclure dans la section conn. La valeur « %any » indique au serveur strongSwan de transmettre l'identité fournie par le client VPN.
auto=add	Ce paramètre indique que cette section de connexion est active. Le serveur BlackBerry 2FA n'utilise pas ce paramètre, mais vous devez l'inclure dans la section conn.

Configuration du fichier eap-radius.conf

Le fichier eap-radius.conf se trouve dans le répertoire /etc/strongswan.d/charon. Il spécifie les détails pour l'authentification d'EAP auprès de RADIUS. Le fichier de configuration par défaut dispose de tous les paramètres que vous devez configurer, mais la plupart sont commentés et certains n'ont pas de valeur attribuée. Vous devez modifier les paramètres requis en supprimant le signe dièse (#) et en définissant leurs valeurs comme décrit dans le tableau suivant.

Paramètre	Description
accounting=no	Ce paramètre empêche strongSwan d'envoyer des informations de comptabilité RADIUS au serveur BlackBerry 2FA.
nas_identifier	Ce paramètre facultatif indique l'élément NAS-Identifier à inclure dans les messages RADIUS. Vous pouvez utiliser ce paramètre si plusieurs serveurs strongSwan utilisent le même serveur BlackBerry 2FA.
port=1812	Ce paramètre indique le port utilisé par le serveur BlackBerry 2FA pour recevoir les demandes RADIUS d'authentification.
secret=<*secret partagé*>	Ce paramètre indique le secret partagé entre strongSwan et le serveur BlackBerry 2FA. Lorsque vous configurez la connectivité de serveur VPN dans le serveur BlackBerry 2FA, vous devez saisir le secret partagé RADIUS que vous indiquez ici.

Paramètre	Description
server=<*adresse IP du serveur VPNAuth*>	Ce paramètre spécifie l'adresse IP ou l'élément FQDN du serveur BlackBerry 2FA.
ike_to_radius=1, 2, 311:1, 311:11, 311:25	Ce paramètre spécifie la liste séparée par des virgules des nombres qui représentent la liste des attributs RADIUS que strongSwan doit transmettre au serveur BlackBerry 2FA. Les nombres séparés par le signe deux points représentent des attributs propres à un fournisseur. Le premier nombre identifie le fournisseur (par exemple, 311 est le nombre correspondant à Microsoft), et le deuxième nombre identifie le type d'attribut. Ce paramètre est dans la section « forward » du fichier de configuration.
radius_to_ike=311:26, 311:17, 311:16	Ce paramètre spécifie la liste de nombres séparés par des virgules qui représentent la liste des attributs RADIUS que le serveur BlackBerry 2FA doit transférer à strongSwan. Les nombres séparés par le signe deux points représentent des attributs propres à un fournisseur. Le premier nombre identifie le fournisseur (par exemple, 311 est le nombre correspondant à Microsoft), et le deuxième nombre identifie le type d'attribut. Ce paramètre est dans la section « forward » du fichier de configuration.

Configuration du serveur BlackBerry 2FA pour se connecter à une passerelle VPN

Avant de commencer : Obtenez l'adresse IP et le secret partagé pour les passerelles VPN.

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Serveur BlackBerry 2FA**.
2. Cliquez sur le serveur BlackBerry 2FA pour lequel vous souhaitez configurer une passerelle VPN.
3. Dans la section **Configuration du VPN**, cliquez sur +.
4. Dans le champ **Nom du serveur VPN**, saisissez un nom unique pour la passerelle VPN à laquelle vous vous connectez.
5. Dans le champ **Hôte VPN**, saisissez l'adresse IP de la passerelle VPN.
6. Dans les champs **Secret partagé** et **Confirmer le secret partagé**, saisissez et confirmez le secret partagé de la passerelle VPN.
7. Si nécessaire, remplacez la configuration d'application BlackBerry 2FA. Vous pouvez configurer les champs suivants indépendamment les uns des autres. Les champs laissés vides sont ignorés et les valeurs par défaut de la section **Invite de terminal par défaut** sont utilisées.
   a) Sélectionnez **Invite BlackBerry 2FA pour ce VPN**.
   b) Dans le champ **Titre**, saisissez le titre que vous voulez que l'application affiche dans son message. Par exemple, « Exemple de VPN d'organisation ».
   c) Dans le champ **Message**, saisissez le message que vous voulez que l'application affiche aux utilisateurs. Ce message explique aux utilisateurs ce qui est attendu d'eux.

d) Dans le champ **Confirmer le texte du bouton**, saisissez le texte qui apparaît sur le bouton sur lequel les utilisateurs peuvent appuyer pour confirmer l'authentification à deux facteurs.
e) Dans le champ **Refuser le texte du bouton**, saisissez le texte qui apparaît sur le bouton sur lequel les utilisateurs peuvent appuyer pour refuser l'authentification à deux facteurs.
f) Dans le champ **Délai (secondes)**, saisissez la durée, en secondes, avant l'expiration de la transaction d'authentification.

8. Cliquez sur **Ajouter**.
9. Répétez ces étapes pour chaque passerelle VPN que vous souhaitez ajouter.
10. Cliquez sur **Enregistrer**.

Mise à jour d'une connexion vers une passerelle VPN

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Serveur BlackBerry 2FA**.
2. Cliquez sur le nom du serveur 2FA que vous souhaitez configurer.
3. Cliquez sur le nom du serveur VPN que vous souhaitez mettre à jour.
4. Mettez à jour la configuration si nécessaire. Pour plus d'informations, reportez-vous aux étapes 4 à 7 de Configuration du serveur BlackBerry 2FA pour se connecter à une passerelle VPN.
5. Cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer**.

Suppression d'une connexion à une passerelle VPN

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Serveur BlackBerry 2FA**.
2. En regard du serveur VPN que vous voulez supprimer, cliquez sur ✕.
3. Cliquez sur **Oui**.
4. Cliquez sur **Enregistrer**.

Configuration de la connexion au point de terminaison d'API REST

Le point de terminaison d'API REST du serveur BlackBerry 2FA est protégé à l'aide de l'élément HTTPS authentifié par le serveur. Vous devez configurer vos services personnalisés afin qu'ils approuvent le serveur BlackBerry 2FA. Vous disposez des options suivantes :

- Vous pouvez utiliser le certificat auto-signé par défaut généré lors de l'installation du serveur BlackBerry 2FA. Le certificat auto-signé par défaut se trouve à l'emplacement bb2fa-config/restkeystore.jks. Votre application cliente doit être configurée pour approuver ce certificat de façon explicite. Le port de serveur par défaut est le port 5443.
- Vous pouvez fournir votre propre certificat signé par une autorité de certification en l'important dans un fichier de clés Java sous l'alias « bb2fa » (RSA 2048 est recommandée comme algorithme de clé). Copiez le fichier de clés dans le répertoire bb2fa-config et mettez à jour son nom et son mot de passe sur la page de configuration du serveur BlackBerry 2FA dans BlackBerry UEM.

Dans tous les cas, les services personnalisés sont authentifiés à l'aide d'une authentification HTTP de base (nom d'utilisateur et mot de passe, qui sont envoyés en tant qu'en-têtes dans la demande).

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Serveur BlackBerry 2FA**.
2. Cliquez sur le nom du serveur 2FA que vous souhaitez configurer.
3. Dans la section **Configuration de l'interface REST**, saisissez les informations.
4. Cliquez sur **Enregistrer**.

Configuration de la connectivité du point de terminaison d'API REST

Pour configurer la connectivité entre les applications clientes et le point de terminaison d'API REST du serveur BlackBerry 2FA, vous devez configurer vos applications clientes afin qu'elles approuvent le serveur BlackBerry 2FA.

Les applications clientes sont authentifiées à l'aide d'une authentification HTTP de base (nom d'utilisateur et mot de passe, qui sont envoyés en tant qu'en-têtes dans la demande). Le point de terminaison d'API REST est protégé à l'aide de l'élément HTTPS authentifié par le serveur (https://*<nom d'hôte>*:*<port>*/*<préfixe>*/). Le port par défaut est 5443 et le préfixe par défaut est « rest ». Les demandes REST suivantes sont prises en charge sur le point de terminaison :

Chemin d'accès	Type	Description	Notes
/*<préfixe>*/twofactor	POST	Demande d'authentification à deux facteurs	

Le message de demande est envoyé à l'aide d'une requête HTTP POST et est au format JSON, avec les paramètres suivants :

Paramètre	Type	Description	Notes
username	Chaine	Nom d'utilisateur	

Paramètre	Type	Description	Notes
Mot de passe	Chaine	Mot de passe utilisateur, ou mot de passe à usage unique et mot de passe utilisateur	Facultatif, en fonction de la stratégie
policy	Nombre entier	Option d'authentification : • 0 : authentification à facteur unique à l'aide d'un mot de passe d'entreprise • 1 : authentification à deux facteurs à l'aide d'un mot de passe d'entreprise • 2 : authentification à deux facteurs à l'aide d'un mot de passe de terminal passif • 3 : authentification à deux facteurs à l'aide d'un mot de passe de terminal actif	
oneTimePassword	Chaine	Mot de passe à usage unique	Facultative
messageTitle	Chaine	Texte du titre de la boite de dialogue	Facultative
message	Chaine	Texte du message de la boite de dialogue	Facultative
confirmButtonText	Chaine	Texte du bouton de confirmation de la boite de dialogue	Facultative
declineButtonText	Chaine	Texte du bouton de refus de la boite de dialogue	Facultative
timeout	Nombre entier	Délai d'expiration de la boite de dialogue (secondes)	Facultative

Le corps du message de réponse est au format JSON, avec le paramètre suivant :

Paramètre	Type	Description	Notes
info	Chaine	Message d'information	

Le message de réponse contient également les codes d'état HTTP suivants :

État	Description	Notes
200	OK	Authentification réussie
400	Demande incorrecte	Paramètres non valides

État	Description	Notes
401	Non autorisé	Échec de l'authentification
403	Refusé	Authentification refusée par l'utilisateur
500	Erreur de serveur interne	Erreur interne

Création d'un client d'API REST dans le serveur BlackBerry 2FA

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Serveur BlackBerry 2FA**.
2. Cliquez sur le nom du serveur 2FA que vous souhaitez configurer.
3. Dans la section **Configuration du client REST**, cliquez sur +.
4. Dans le champ **Nom du client REST**, saisissez un nom convivial pour le client.
5. Dans le champ **ID du client REST** , saisissez un nom pour le client qui sera associé au mot de passe.
6. Dans le champ **Mot de passe**, saisissez un mot de passe. Il doit comporter au moins huit caractères
7. Dans le champ **Confirmer le mot de passe**, saisissez une seconde fois le mot de passe.
8. Cliquez sur **Ajouter**.
9. Répétez ces étapes pour chaque client que vous souhaitez ajouter.
10. Cliquez sur **Enregistrer**.

Autorisation de l'authentification MS-CHAP pour les utilisateurs d'un domaine

Vous pouvez autoriser un serveur BlackBerry 2FA à prendre en charge les authentifications MS-CHAPv1 et MS-CHAPv2 pour les demandes RADIUS (par exemple, les demandes provenant d'une passerelle VPN) pour les utilisateurs qui sont membres du domaine sélectionné. Le domaine est disponible pour cette option car le serveur 2FA est exécuté sur un hôte associé à un domaine Active Directory auquel BlackBerry UEM est également connecté.

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Serveur BlackBerry 2FA**.
2. Cliquez sur le nom du serveur 2FA que vous souhaitez configurer.
3. Dans la section **Configuration Active Directory**, sélectionnez le domaine pour lequel vous souhaitez activer l'authentification MS-CHAP. Pour désactiver l'authentification MS-CHAP, désélectionnez le domaine.
4. Cliquez sur **Enregistrer**.

Configuration de l'application BlackBerry 2FA

Vous pouvez personnaliser le message par défaut affiché par BlackBerry 2FA pour les utilisateurs lorsqu'ils se connectent à vos ressources. Vous pouvez également définir la durée, en secondes, avant l'expiration de l'invite d'authentification.

Vous pouvez également remplacer ces paramètres pour chaque passerelle VPN que vous configurez. Pour plus d'informations sur la configuration de passerelles VPN, reportez-vous à Configuration du serveur BlackBerry 2FA pour se connecter à une passerelle VPN.

1. Dans la console de gestion BlackBerry UEM, sur la barre de menus, cliquez sur **Paramètres** > **Intégration externe** > **Serveur BlackBerry 2FA**.
2. Cliquez sur le nom du serveur 2FA que vous souhaitez configurer.
3. Dans la section **Invite de terminal par défaut**, procédez comme suit :
   a) Dans le champ **Titre**, saisissez le titre que vous voulez que l'application affiche dans son message. Par exemple, « Exemple de VPN d'organisation ».
   b) Dans le champ **Message**, saisissez le message que vous voulez que l'application affiche aux utilisateurs. Ce message explique aux utilisateurs ce qui est attendu d'eux.
   c) Dans le champ **Confirmer le texte du bouton**, saisissez le texte qui apparaît sur le bouton sur lequel les utilisateurs peuvent appuyer pour confirmer l'authentification à deux facteurs.
   d) Dans le champ **Refuser le texte du bouton**, saisissez le texte qui apparaît sur le bouton sur lequel les utilisateurs peuvent appuyer pour refuser l'authentification à deux facteurs.
   e) Dans le champ **Délai (secondes)**, saisissez la durée, en secondes, avant l'expiration de la transaction d'authentification.
4. Cliquez sur **Enregistrer**.

Attribution d'une configuration d'une passerelle VPN ou d'un client REST à un groupe d'utilisateurs

Pour autoriser les utilisateurs à utiliser des clients VPN ou REST, vous devez attribuer une configuration de passerelle VPN ou de client REST à des groupes d'utilisateurs. Vous pouvez créer des groupes comprenant les utilisateurs auxquels vous souhaitez attribuer les configurations. Les utilisateurs peuvent uniquement utiliser les configurations qui leur sont attribuées.

Avant de commencer : Effectuez l'une des opérations suivantes :

- Configuration du serveur BlackBerry 2FA pour se connecter à une passerelle VPN
- Création d'un client d'API REST dans le serveur BlackBerry 2FA

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Groupes** > **Utilisateurs** sur la barre de menu.
2. Créez un groupe ou cliquez sur le nom du groupe auquel vous voulez attribuer une configuration.
3. Cliquez sur l'onglet **BlackBerry 2FA**.
4. Cliquez sur +.
5. Choisissez une configuration de terminal client dans la liste déroulante.
6. Cliquez sur **Attribuer**.

Installez l'application BlackBerry 2FA sur les terminaux

BlackBerry 2FA est disponible pour les terminaux iOS, Android et BlackBerry 10.

Terminaux iOS et Android

Pour les terminaux iOS et Android, les fonctionnalités BlackBerry 2FA sont incluses dans l'application BlackBerry UEM Client. Les utilisateurs doivent télécharger l'élément BlackBerry UEM Client pour activer leur terminal avec BlackBerry UEM pour utiliser 2FA.

Les utilisateurs peuvent télécharger l'application BlackBerry UEM Client sur Google Play et sur l'App Store.

Terminaux BlackBerry 10

Pour les terminaux BlackBerry 10, vous devez envoyer l'application BlackBerry 2FA aux terminaux en utilisant BlackBerry UEM. Effectuez les opérations suivantes avec BlackBerry UEM :

- Si nécessaire, utilisez la console de gestion BlackBerry UEM pour spécifier un emplacement réseau partagé pour les applications internes.
- Dans la console de gestion BlackBerry UEM, ajoutez le fichier d'application BlackBerry 2FA (.bar) en tant qu'application interne. L'application BlackBerry 2FA se trouve ici : https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B
- Dans la console de gestion BlackBerry UEM, attribuez l'application à des comptes d'utilisateur ou à des groupes.

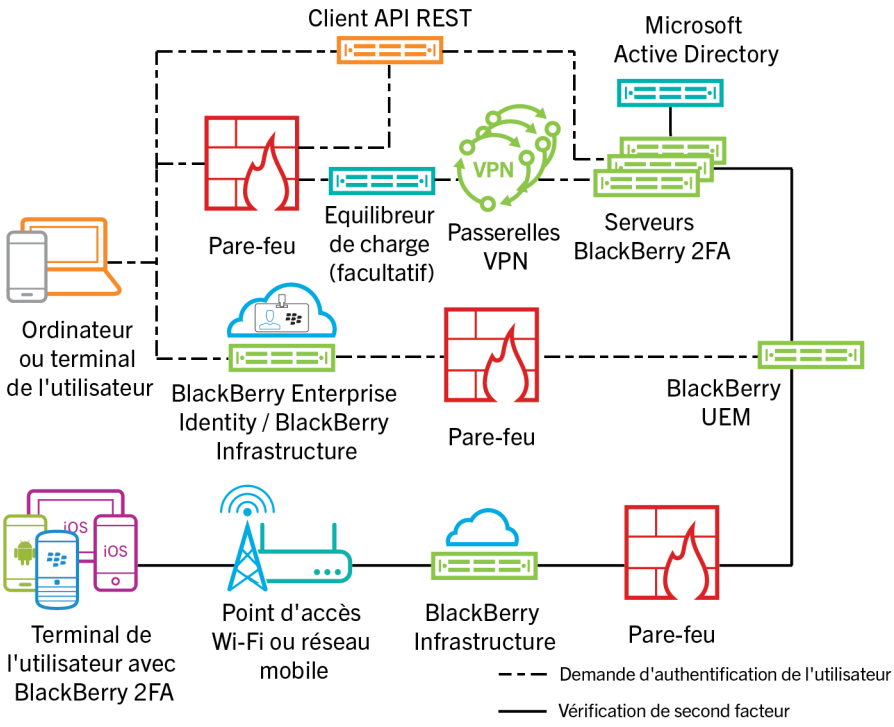
Pour les terminaux dotés d'un espace Travail, l'application est installée dans l'espace Travail. Les utilisateurs peuvent aussi l'installer à l'aide de BlackBerry World pour Travail si vous n'effectuez pas l'installation obligatoire.

Pour plus d'informations sur l'envoi d'applications, consultez le contenu relatif à l'administration de BlackBerry UEM.

Architecture : haute disponibilité de BlackBerry 2FA

BlackBerry 2FA prend en charge la haute disponibilité active-active. Vous pouvez installer plusieurs instances du serveur BlackBerry 2FA afin de garantir l'équilibrage de charge pour les demandes d'authentification et afin de promouvoir la fiabilité.

Le schéma suivant illustre un scénario de haute disponibilité. Certaines solutions VPN peuvent inclure un équilibrage de charge, et dans ce scénario, aucun équilibrage de charge supplémentaire n'est nécessaire.



Configuration du serveur BlackBerry 2FA pour la haute disponibilité

Vous pouvez utiliser les mêmes ports pour tous les serveurs BlackBerry 2FA.

Pour maintenir le chiffrement unique des informations de configuration, il est recommandé de ne pas copier le fichier bb2fa-config.json entre les serveurs BlackBerry 2FA. Vous devez configurer chaque serveur séparément dans la console de gestion BlackBerry UEM.

Tâche	Description
1	Si vous ne l'avez pas déjà fait, configurez la haute disponibilité de votre passerelle VPN. Pour plus d'informations, consultez la documentation de votre passerelle VPN.

Tâche	Description
2	Installez au moins deux serveurs BlackBerry 2FA. Pour chaque serveur, générez et téléchargez un fichier d'activation. Lors des installations ultérieures, vous pouvez choisir de ne pas sélectionner les fichiers d'application BlackBerry 2FA. Vous n'avez pas besoin d'installer les fichiers plus d'une fois. Pour plus d'informations, consultez le contenu relatif à l'installation et à la mise à niveau de BlackBerry 2FA.
3	Créez un profil pour les serveurs BlackBerry 2FA sur le serveur VPN. Pour plus d'informations, reportez-vous à Configuration d'une connexion entre le serveur BlackBerry 2FA et une passerelle VPN.
4	Connectez chaque serveur BlackBerry 2FA à une passerelle VPN. Pour plus d'informations, reportez-vous à Configuration du serveur BlackBerry 2FA pour se connecter à une passerelle VPN.
5	Configuration de la connexion au point de terminaison d'API REST
6	Création d'un client d'API REST dans le serveur BlackBerry 2FA.
7	Autorisation de l'authentification MS-CHAP pour les utilisateurs d'un domaine
8	Configuration de l'application BlackBerry 2FA
9	Attribution d'une configuration d'une passerelle VPN ou d'un client REST à un groupe d'utilisateurs
10	Si nécessaire, envoyez l'application BlackBerry 2FA aux terminaux. Pour plus d'informations, reportez-vous à Installez l'application BlackBerry 2FA sur les terminaux.
11	
12	

Journalisation et rapports

BlackBerry 2FA stocke ses fichiers journaux dans <*install_dir*>\logs. Il existe quatre fichiers journaux :

- bb2fa.log est le principal fichier journal qui contient tous les messages que le serveur BlackBerry 2FA écrit. Par exemple, il comprend des messages de démarrage et d'arrêt relatifs à la progression de l'authentification.
- key_log.txt est le fichier qui contient les messages relatifs à la création et à l'état des clés que le serveur BlackBerry 2FA exige pour protéger les informations sensibles, telles que les mots de passe.
- bb2fa-audit.log est un fichier d'audit séparé par des virgules qui enregistre chaque demande d'authentification émise par le serveur BlackBerry 2FA.
- winrun_log.txt est le fichier qui contient les messages propres au démarrage et à l'exécution du serveur BlackBerry 2FA lorsque vous l'exécutez dans les services Windows.

BlackBerry 2FA utilise l'outil de journalisation Apache log4j. Par défaut, le serveur BlackBerry 2FA écrit les messages de journalisation au niveau Informations.

Le serveur BlackBerry 2FA crée un fichier journal et un fichier d'audit chaque jour. Lorsque le fichier journal ou d'audit est créé, le fichier journal ou d'audit précédent est horodaté comme bb2fa.<*date*>.log ou b2fa-audit.log.<*date*>.

Vous pouvez modifier le niveau de journalisation et l'emplacement où BlackBerry 2FA stocke les fichiers journal et d'audit à l'aide du fichier log4j.properties dans <*install_dir*>\bb2fa-config. Pour plus d'informations, rendez-vous sur http://logging.apache.org/log4j/2.x/ et consultez le *guide d'utilisateur de Apache log4j 2*.

Audit des demandes d'authentification

Serveur BlackBerry 2FA

Le serveur BlackBerry 2FA enregistre chaque demande d'authentification qu'il émet dans un fichier journal lorsque la demande expire. Le fichier journal d'audit comprend les informations suivantes sur chaque demande :

- Date
- Heure
- ID de transaction
- Nom du client
- Adresse IP du client
- Nom d'utilisateur
- Option d'authentification
- Terminaux BlackBerry 10 attribués à l'utilisateur
- Terminaux tiers attribués à l'utilisateur
- Terminaux de système d'exploitation BlackBerry attribués à l'utilisateur
- Terminal qui a répondu à la demande d'authentification
- Temps (en secondes) nécessaire pour faire aboutir la demande d'authentification
- Résultat de la demande

Par exemple :

```
2015-11-05,13:27:17.822,50dbe1cc,radtest,10.135.41.74,caperez,ENTERPRISE_PW,
[BESNameOne:BB10:2fff369:OK],[BES12-TEST:THIRDPARTY: 1fdf6d37-4f21-4516-b43f-
c90be83f646c:OK],[BESNameOne:BBOS:2fff367:OK],[BBOS:2fff367],6.742,AUTH_SUCCEEDED
```

Le fichier journal d'audit est un fichier séparé par des virgules que vous pouvez ouvrir dans n'importe quel logiciel prenant en charge le format CSV. Il est nommé bb2fa-audit.log et est stocké dans <*install_dir*>\logs.

BlackBerry UEM

Pour obtenir des informations sur la journalisation BlackBerry UEM, reportez-vous au contenu relatif à l'administration de BlackBerry UEM.

Centralisation de la journalisation ou de l'audit à l'aide de syslog

Vous pouvez configurer le serveur BlackBerry 2FA de manière à ce qu'il écrive ses fichiers journaux, ses fichiers d'audit ou les deux dans un serveur syslog centralisé plutôt que dans des fichiers locaux.

Remarque : Cette tâche présente un moyen de centraliser la journalisation. Pour plus d'informations sur la façon de configurer la journalisation, rendez-vous sur http://logging.apache.org/log4j/2.x/ et consultez le *guide de l'utilisateur Apache log4j 2*.

1. Accédez au dossier `<install_dir>\bb2fa-config`.
2. Accédez au dossier `<install_dir>/bb2fa-config`.
3. Sauvegardez le fichier log4j.properties.
4. Ouvrez le fichier log4j.properties dans un éditeur de texte.
5. Pour envoyer des messages à un serveur syslog central, effectuez les actions suivantes :
   a) Modifiez la valeur de `log4j.rootLogger` en l'un des éléments suivants :
      - Pour écrire des messages de journalisation uniquement sur un serveur syslog, `ALL, syslog`
      - Pour écrire des messages de journalisation en local et sur un serveur syslog, `ALL, logfile, syslog`
   b) Ajoutez les lignes suivantes :

```
log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.SYSLOG.Threshold=INFO
log4j.appender.SYSLOG.syslogHost=<hostname>:<port>
log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
log4j.appender.SYSLOG.layout.ConversionPattern=[%-5p] %c - %m%n
```

   c) Définissez la valeur de `log4j.appender.syslog.syslogHost` sur le nom de l'hôte et le port de votre serveur syslog.
   d) Si nécessaire, pour supprimer la journalisation locale, supprimez les lignes suivantes :

```
# Sortie de fichier journal
log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
log4j.appender.logfile.layout.ConversionPattern=%d{ISO8601} [%-5p] (%t) %c -
 %m%n
log4j.appender.logfile.datePattern='.'yyyy-MM-dd
log4j.appender.logfile.Threshold = INFO
log4j.appender.logfile.append=true
log4j.appender.logfile.File=logs/bb2fa.log
```

6. Pour envoyer des messages d'audit à un serveur syslog central, effectuez les actions suivantes :
   a) Modifiez la valeur de `log4j.logger.auditLogger` en l'un des éléments suivants :
      - Pour écrire des messages d'audit uniquement sur un serveur syslog, `ALL, auditsyslog`
      - Pour écrire des messages d'audit en local et sur un serveur syslog, `ALL, auditfile, auditsyslog`
   b) Ajoutez les lignes suivantes :

```
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
log4j.appender.auditsyslog.syslogHost=<hostname>:<port>
```

```
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

c) Définissez la valeur de `log4j.appender.syslog.syslogHost` sur le nom de l'hôte et le port de votre serveur syslog. Vous devez utiliser deux ports distincts pour le fichier d'audit et le fichier journal.

d) Si nécessaire, pour supprimer l'audit en local, supprimez les lignes suivantes :

```
# Sortie de fichier d'audit
log4j.appender.auditfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.auditfile.layout=org.apache.log4j.PatternLayout
log4j.appender.auditfile.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
log4j.appender.auditfile.datePattern='.'yyyy-MM-dd
log4j.appender.auditfile.Threshold = INFO
log4j.appender.auditfile.append=true
log4j.appender.auditfile.File=logs/bb2fa-audit.log
```

7. Enregistrez vos modifications.
8. Dans les services Windows, redémarrez le service BlackBerry 2FA.
9. Redémarrez le service BlackBerry 2FA.

Exemple de fichier log4j.properties avec une journalisation en local et sur syslog

```
log4j.rootLogger=ALL, logfile, syslog

log4j.logger.auditLogger=ALL, auditfile, auditsyslog

# Nous voulons contrôler les sorties Apache CFX ete Jetty,
# qui présentent des caractéristiques de verbose au niveau DEBUG
log4j.logger.org.apache.cxf=INFO
log4j.logger.org.eclipse.jetty=INFO

# Rediriger les journaux vers un fichier journal local
log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
log4j.appender.logfile.layout.ConversionPattern=%d{ISO8601} [%-5p] (%t) %c - %m%n
log4j.appender.logfile.datePattern='.'yyyy-MM-dd
log4j.appender.logfile.Threshold = INFO
log4j.appender.logfile.append=true
log4j.appender.logfile.File=logs/bb2fa.log

# Rediriger les journaux vers un serveur syslog distant
log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.syslog.Threshold = INFO
log4j.appender.syslog.syslogHost=syslog.example.com:514
log4j.appender.syslog.layout=org.apache.log4j.PatternLayout
log4j.appender.syslog.layout.ConversionPattern=[%-5p] %c - %m%n

# Rediriger les messages d'audit vers un fichier d'audit en local
log4j.appender.auditfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.auditfile.layout=org.apache.log4j.PatternLayout
log4j.appender.auditfile.layout.ConversionPattern=%d{yyyy-MM-dd},%d{HH:mm:ss.SSS},
%m%n
log4j.appender.auditfile.datePattern='.'yyyy-MM-dd
log4j.appender.auditfile.Threshold = INFO
log4j.appender.auditfile.append=true
log4j.appender.auditfile.File=logs/bb2fa-audit.log
```

```
# Rediriger les messages d'audit vers un serveur syslog distant
#(vous avez besoin d'un autre port pour générer un fichier différent)
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
log4j.appender.auditsyslog.syslogHost=syslog.example.com:515
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

Options d'authentification

BlackBerry 2FA propose les options d'authentification suivantes :

Remarque : Si un utilisateur se voit attribuer une option à deux facteurs, il est automatiquement autorisé à utiliser un jeton OTP s'il s'en voit attribuer un.

Option d'authentification	Description	Utile dans les cas suivants :
Authentification à deux facteurs à l'aide d'un mot de passe d'entreprise	Lorsqu'un utilisateur se connecte, il fournit un nom d'utilisateur et un mot de passe de répertoire, puis il reçoit une invite de confirmation de la demande d'authentification sur le terminal. Si un utilisateur se voit attribuer cette option, il est automatiquement autorisé à utiliser un jeton OTP s'il s'en voit attribuer un. Cette option est prise en charge sur tous les terminaux.	Votre organisation considère la sécurité comme l'objectif le plus important d'un déploiement.
Authentification à deux facteurs à l'aide d'un mot de passe de terminal passif	Lorsqu'un utilisateur se connecte, il fournit uniquement un nom d'utilisateur, puis reçoit une invite de confirmation de la demande d'authentification. Si le terminal est verrouillé, l'utilisateur doit fournir le mot de passe du terminal avant de pouvoir confirmer l'invite. Si un utilisateur se voit attribuer cette option, il est automatiquement autorisé à utiliser un jeton OTP s'il s'en voit attribuer un. Pour les terminaux BlackBerry 10, les utilisateurs doivent fournir le mot de passe de l'espace Travail si ce dernier est verrouillé. Cette option est prise en charge sur tous les terminaux.	Votre organisation considère la convivialité comme l'objectif le plus important d'un déploiement.

Option d'authentification	Description	Utile dans les cas suivants :
Authentification à deux facteurs à l'aide d'un mot de passe de terminal actif	Lorsqu'un utilisateur se connecte, il ne fournit qu'un nom d'utilisateur, puis il reçoit une invite de confirmation de la demande d'authentification sur son terminal. L'utilisateur doit toujours fournir le mot de passe du terminal pour pouvoir confirmer l'invite. Si un utilisateur se voit attribuer cette option, il est automatiquement autorisé à utiliser un jeton OTP s'il s'en voit attribuer un. Pour les terminaux BlackBerry 10, les utilisateurs doivent fournir le mot de passe de l'espace Travail. Cette option est prise en charge uniquement pour les terminaux sous les systèmes d'exploitation BlackBerry 10 et BlackBerry (version 6.0 à 7.1).	Votre organisation met l'accent sur la convivialité, mais veut se protéger contre l'éventualité qu'une personne prenne un terminal déverrouillé et accepte l'invite du terminal.
Authentification à facteur unique à l'aide d'un mot de passe d'entreprise	Les utilisateurs se connectent à l'aide de l'authentification Microsoft Active Directory uniquement.	• L'utilisateur ne possède pas de terminal. • L'utilisateur a oublié ou perdu son terminal. • L'utilisateur n'a pas besoin d'utiliser une authentification à deux facteurs.

Remarque : Dans BlackBerry 2FA version 2.5, vous pouvez configurer les options d'authentification d'utilisateur de différentes manières. Par défaut, les options d'authentification sont configurées à l'aide d'un profil BlackBerry 2FA dans BlackBerry UEM. Cependant, vous pouvez modifier cette configuration par défaut pour les demandes d'authentification envoyées via l'API REST, les passerelles VPN et d'autres clients RADIUS. Pour plus d'informations, reportez-vous à Configuration de la connectivité du point de terminaison d'API REST ou Configuration d'une connexion entre le serveur BlackBerry 2FA et une passerelle VPN.

Noms d'utilisateur, mots de passe et répertoires

BlackBerry 2FA authentifie les utilisateurs qui sont disponibles dans un répertoire. Les serveurs BlackBerry 2FA et BlackBerry UEM sont connectés à ces répertoires. En fonction de la configuration de ces connexions, BlackBerry 2FA prend en charge quatre types d'utilisateur :

- Utilisateurs dans un domaine Microsoft Active Directory connecté à la fois à un serveur BlackBerry 2FA et à BlackBerry UEM
- Utilisateurs dans un domaine Microsoft Active Directory non connecté à un serveur BlackBerry 2FA mais connecté à BlackBerry UEM
- Utilisateurs dans un répertoire LDAP connecté à BlackBerry UEM
- Utilisateurs dans un répertoire BlackBerry UEM local

Lorsqu'un utilisateur se connecte, il doit fournir un nom d'utilisateur, et éventuellement un mot de passe.

Nom d'utilisateur

Le nom d'utilisateur doit correspondre à une entrée utilisateur unique dans un répertoire. Si l'utilisateur ne peut pas être résolu de manière unique, une demande d'authentification échouerait. Pour spécifier le répertoire dans lequel réside l'utilisateur, ce dernier doit être identifié conformément aux noms d'utilisateur suivants pour chaque type d'utilisateur :

- Les noms d'utilisateur suivants sont pris en charge pour les utilisateurs dans un domaine Microsoft Active Directory connecté à la fois à un serveur BlackBerry 2FA et à BlackBerry UEM. Ces utilisateurs peuvent s'authentifier à l'aide de PAP, MSCHAPv1, MSCHAPv2 et EAP-MSCHAPv2, et peuvent être configurés pour utiliser des groupes d'autorisations pour chaque client d'API REST,ainsi que des groupes de remplacements d'authentification pour chaque passerelle VPN.

  <nom d'utilisateur> (par exemple, jsmith)

  <nom d'utilisateur>@<nom de domaine NetBIOS> (par exemple, jsmith@company)

  <nom de domaine NetBIOS>\<nom d'utilisateur> (par exemple, company\jsmith)

  <adresse électronique> (par exemple, jsmith@company.com)
- Les noms d'utilisateur suivants sont pris en charge pour les utilisateurs dans un domaine Microsoft Active Directory qui n'est pas connecté à un serveur BlackBerry 2FA, mais connecté à BlackBerry UEM. Ces utilisateurs peuvent s'authentifier uniquement à l'aide de PAP.

  <nom d'utilisateur> (par exemple, jsmith)

  <nom d'utilisateur>@<nom de domaine NetBIOS> (par exemple, jsmith@company)

  <nom de domaine NetBIOS>\<nom d'utilisateur> (par exemple, company\jsmith)

  <adresse électronique> (par exemple, jsmith@company.com)
- Les noms d'utilisateur suivants sont pris en charge pour les utilisateurs dans un répertoire LDAP connecté à BlackBerry UEM. Ces utilisateurs doivent s'authentifier avec PAP.

  Remarque : Le serveur BlackBerry 2FA ne peut pas se connecter à ce répertoire.

  <nom d'utilisateur> (par exemple, jsmith)

  <nom d'utilisateur>@<répertoire FQDN> (par exemple, jsmith@company.ldap.net)

  <répertoire FQDN>\<nom d'utilisateur> (par exemple, company.ldap.net\jsmith)

  <adresse électronique> (par exemple, jsmith@company.com)
- Les noms d'utilisateur suivants sont pris en charge pour les utilisateurs dans un répertoire BlackBerry UEM local. Ces utilisateurs doivent s'authentifier avec PAP.

  Remarque : Le serveur BlackBerry 2FA ne peut pas se connecter à ce répertoire.

  <nom d'utilisateur> (par exemple, jsmith)

<nom d'utilisateur>@local (par exemple, jsmith@local)

local\<nom d'utilisateur> (par exemple, local\jsmith)

<adresse électronique> (par exemple, jsmith@company.com)

Mot de passe

Lorsqu'un utilisateur se connecte, il doit fournir un mot de passe de répertoire en fonction de l'option d'authentification que sa configuration lui impose d'utiliser.

Si un utilisateur s'authentifie à l'aide d'un jeton de mot de passe à usage unique (OTP), il doit fournir le jeton OTP et son mot de passe de répertoire, quelle que soit l'option d'authentification à deux facteurs que sa configuration lui impose d'utiliser.

- Pour se connecter à un réseau VPN, l'utilisateur doit saisir le jeton OTP et le mot de passe de répertoire dans le champ de mot de passe. Le jeton OTP est saisi en premier, suivi par le mot de passe de répertoire, et aucun espace ou séparateur ne peut être ajouté.
- Lors d'une connexion à partir d'un client connecté à une API REST, l'utilisateur doit saisir le mot de passe de répertoire dans le champ de mot de passe, puis saisir le jeton OTP dans un champ dédié.

Point de terminaison d'API REST

Le serveur BlackBerry 2FA dispose d'un point de terminaison d'API REST externe qui étend BlackBerry 2FA à des services personnalisés, comme des applications web et des applications clientes SIP. Vous pouvez utiliser la page de configuration du serveur BlackBerry 2FA dans la console de gestion BlackBerry UEM pour créer un client REST. Pour plus d'informations, reportez-vous à Configuration de la connectivité du point de terminaison d'API REST.

Passerelles VPN

Vous pouvez utiliser la page de configuration du serveur BlackBerry 2FA dans la console de gestion BlackBerry UEM pour créer une connexion à une passerelle VPN. La connexion entre une passerelle VPN et le serveur BlackBerry 2FA est établie à l'aide de RADIUS. Pour plus d'informations, reportez-vous à Configuration d'une connexion entre le serveur BlackBerry 2FA et une passerelle VPN.

Glossaire

API	interface de programmation d'application
CA	certification authority (autorité de certification)
DNS	Domain Name System (système DNS)
ECDH	Elliptic Curve Diffie-Hellman (courbe éliptique Diffie-Hellman)
EAP	Extensible Authentication Protocol (protocole d'authentification extensible)
EMM	Enterprise Mobility Management (Gestion de la mobilité d'entreprise)
FQDN	Fully Qualified Domain Name (nom de domaine complet)
HTTP	Hypertext Transfer Protocol (protocole de transfert hypertexte)
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IP	Internet Protocol (protocole Internet)
stratégie informatique	Une stratégie informatique est composée de diverses règles qui contrôlent les fonctions de sécurité et le comportement des terminaux.
IKE	Internet Key Exchange (protocole IKE)
MAM	mobile application management (Gestion des applications mobiles)
MDM	Mobile device management (gestion des terminaux mobiles)
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol (protocole d'authentification par challenge de Microsoft)
NAS	Network-attached storage (système de stockage en réseau)
NTLM	NT LAN Manager
OTP	One-time password (mot de passe à usage unique)

PAP	Push Access Protocol (protocole PAP)
RADIUS	Remote Authentication Dial In User Service (service utilisateur de connexion par authentification à distance)
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol (protocole d'initialisation de session)
SSL	Secure Sockets Layer (protocole SSL)
TLS	Transport Layer Security (sécurité de la couche de transport)
UEM	Unified Endpoint Manager
VPN	Virtual Private Network (réseau privé virtuel)

Informations juridiques

COMME ENSEMBLE DEHORS AU-DESSUS, MAIS PEUVENT ÊTRE LIMITÉES, SONT LIMITÉES À QUATRE-VINGT-DIX 90 JOURS À PARTIR DE LA DATE QUE VOUS AVEZ ACQUIS TOUT D'ABORD LA DOCUMENTATION OU LA ORDRE DU JOUR QUI FAIT L'OBJET DE LA RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI APPLICABLE DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY SERA RESPONSABLE POUR TOUT TYPE DE DOMMAGES LIÉS À CETTE DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU L'INEXÉCUTION DE TOUT LOGICIEL, MATÉRIEL, SERVICE, OU TOUT TIERS PRODUITS ET SERVICES MENTIONNÉS AUX PRÉSENTES Y COMPRIS SANS LIMITATION LES DOMMAGES SUIVANTS : DOMMAGE DIRECT, CONSÉCUTIF, EXEMPLAIRE, FORTUIT, INDIRECT, SPÉCIAL, PUNITIF OU AGGRAVÉE, DOMMAGES-INTÉRÊTS POUR PERTE DE PROFITS OU DE REVENUS, ÉCHEC DE RÉALISER TOUT PRÉVU DES ÉCONOMIES, INTERRUPTION D'ACTIVITÉ, PERTES D'INFORMATIONS COMMERCIALES, PERTE D'OPPORTUNITÉ COMMERCIALE, DE CORRUPTION OU DE PERTE DE DONNÉES, PANNES POUR TRANSMETTRE OU RECEVOIR N'IMPORTE QUEL DA TA, PROBLÈMES LIÉS À TOUTES LES APPLICATIONS UTILISANT EN CONJONCTION AVEC BLACKBERRY PRODUITS OU SERVICES, DURÉE D'INDISPONIBILITÉ DES COÛTS, PERTE D'USAGE DU BLACKBERRY, PRODUITS, SERVICES OU TOUTE PARTIE DE CELLE-CI OU DE TOUT SERVICE DE TEMPS D'ANTENNE, COÛT DE MARCHANDISES DE REMPLACEMENT, LES COÛTS DE COUVERTURE, INSTALLATIONS OU SERVICES, COÛT DU CAPITAL OU AUTRES PERTES PÉCUNIAIRES SEMBLABLES, SI CES DOMMAGES ONT ÉTÉ PRÉVUES OU IMPRÉVUES, ET MÊME SI LE BLACKBERRY A ÉTÉ AVISÉ DE LA DEMAND Y DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI APPLICABLE DANS VOTRE JURIDICTION, BLACKBERRY N'AURA AUCUNE AUTRE OBLIGATION, OBLIGATION OU RESPONSABILITÉ QUE CE SOIT EN CONTRAT, UN TORT, OU AUTREMENT VOUS Y COMPRIS TOUTE RESPONSABILITÉ POUR NÉGLIGENCE OU STRICT RESPONSABILITÉ CIVILE.

LES LIMITATIONS ET EXCLUSIONS CI-DESSUS SERONT APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DEMANDE OU ACTION PAR VOUS, Y COMPRIS MAIS NON LIMITÉ À B PORTÉE DE CONTRAT, NÉGLIGENCE, RESPONSABILITÉ DÉLICTUELLE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE JURIDIQUE ET DOIVENT SURVIVRE À UNE INEXÉCUTION FONDAMENTALE OU BRE DOULEURS OU L'ÉCHEC DE L'OBJECTIF ESSENTIEL DU PRÉSENT ACCORD OU DE TOUTE MESURE CORRECTIVE QU'IL CONTIENT ; ET (B) À BLACKBERRY ET SES SOCIÉTÉS AFFILIÉES, LEURS SUCCESSEURS, LES AYANTS DROIT, LES AGENTS, LES FOURNISSEURS (Y COMPRIS LES TEMPS D'ANTENNE SERVICE P ROVIDERS), DISTRIBUTEURS DE BLACKBERRY (Y COMPRIS LES FOURNISSEURS DE SERVICES DE TEMPS D'ANTENNE) AGRÉÉS ET LEURS DIRECTEURS RESPECTIFS, EMPL OYEES ET LES ENTREPRENEURS INDÉPENDANTS.

OUTRE LES LIMITATIONS ET EXCLUSIONS VISÉES CI-DESSUS, EN AUCUN CAS, N'IMPORTE QUEL DIRIGEANT, EMPLOYÉ, AGENT, DISTRIBUTEUR, FOURNISSEUR, ENTREPRENEUR INDÉPENDANT DE BLACKBERRY OU TOUT AFFILIÉ DE BLACKBERRY A TOUTE RESPONSABILITÉ DÉCOULANT D'OU LIÉS À LA DOCUMENTATION.

Avant de souscrire pour, installant ou utilisant des produits tiers et les Services, il est de votre responsabilité de vous assurer que votre fournisseur de service de temps d'antenne a accepté de prend en charge toutes leurs fonctionnalités. Certains fournisseurs de services de temps d'antenne ne pourraient pas offrir fonctionnalité de navigation Internet avec un abonnement à le BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services pour la disponibilité, des arrangements, des plans de service et des caractéristiques de l'itinérance. Installation ou l'utilisation des Services et produits tiers avec les produits et les services de BlackBerry peut exiger un ou plusieurs brevets, marque, droit d'auteur, ou d'autres licences afin d'éviter la contrefaçon ou violation des droits de tiers. Vous êtes seul responsable de déterminer s'il faut utiliser des produits tiers, et Services, si les licences de tiers sont tenus de le faire. Si vous êtes responsable de l'acquisition. Vous ne devriez pas installer ou utiliser les Services et produits tiers jusqu'à ce que toutes les autorisations nécessaires ont été acquis. Tous les produits de tiers et les Services qui sont fournis avec les produits et les services de BlackBerry sont fournis à titre utilitaire à vous et sont fournis « Tel quel » avec aucune conditions implicites ou explicites, endossements, garanties, représentations ou garantie d'aucune genre de BlackBerry et BlackBerry n'assume aucune responsabilité quelle qu'elle soit, en relation avec celui-ci. Votre utilisation des Services et des produits de tiers est régie par et sous réserve de vous acceptant les conditions de licen séparé SSE et autres accords applicables s'y rapportant avec les tierces parties, sauf dans la mesure expressément couverte par une licence ou d'autre accord avec BlackBerry.

Les conditions d'utilisation de tout produit BlackBerry ou service figurent dans une licence distincte ou de toute autre entente avec BlackBerry applicables s'y rapportant. RIEN DANS LA PRÉSENTE DOCUMENTATION VISE À REMPLACER TOUTE ENTENTE ÉCRITE EXPRESSE OU GARANTIES FOURNIES PAR BLACKBERRY POUR UNE PARTIE DE N'IMPORTE QUEL BLACKBERRY PRODUIT OU SERVICE AUTRE QUE DE CETTE DOCUMENTATION.

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

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

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