BlackBerry Enterprise Identity

Guide d'administration

Table des matières

Qu'est-ce que BlackBerry Enterprise Identity ?

BlackBerry Enterprise Identity fournit une authentification à certaines applications Web BlackBerry telles que la console de gestion BlackBerry UEM Cloud et BlackBerry Persona Mobile. BlackBerry Enterprise Identity fournit également une identification unique (SSO) à des services cloud tels que Microsoft Office 365, G Suite, BlackBerry Workspaces et bien d'autres encore. L'identification unique évite aux utilisateurs d'effectuer de nombreuses connexions ou de retenir de nombreux mots de passe. Les administrateurs peuvent également ajouter des services personnalisés à Enterprise Identity pour offrir aux utilisateurs un accès aux applications internes. Les utilisateurs peuvent accéder aux services à partir de n'importe quel terminal qu'ils souhaitent utiliser, tels que des terminaux iOS, Android ou BlackBerry 10 et autres plateformes informatiques.

Enterprise Identity est fourni avec BlackBerry UEM et BlackBerry UEM Cloud. Les administrateurs utilisent la console BlackBerry UEM ou BlackBerry UEM Cloud pour ajouter des services, gérer les utilisateurs, mais également ajouter et gérer des administrateurs supplémentaires. L'intégration avec les produits de gestion de la mobilité d'entreprise BlackBerry facilite la gestion des utilisateurs et des autorisations d'accès aux services en nuage depuis leurs terminaux.

Pour utiliser Enterprise Identity vous devez acheter des licences utilisateur pour les éditions Collaboration, Application ou Contenu de BlackBerry Enterprise Mobility Suite, ou des licences utilisateur BlackBerry Enterprise Identity séparées. Pour plus d'informations sur BlackBerry Enterprise Identity, y compris sur le mode d'achat de Enterprise Identity, consultez les informations sur blackberry.com.

Les navigateurs suivants sont pris en charge pour l'administration : Internet Explorer 11, Google Chrome, Mozilla Firefox et Safari. L'utilisation du client est prise en charge sur tous les navigateurs ci-dessus, ainsi que sur les navigateurs natifs des terminaux exécutant BlackBerry 10 OS version 10.2.1 ou ultérieure, iOS version 8 ou ultérieure et Android version 4.0 ou ultérieure.

Fonctionnalité	Avantage
Améliorer la productivité des employés	Les employés peuvent utiliser un seul mot de passe pour tous les services en nuage, sur tous les terminaux mobiles (iOS, Android et BlackBerry) et les plateformes informatiques traditionnelles (Windows et macOS). Cela permet d'éliminer la frustration provenant de l'utilisation de plusieurs identifiants et mots de passe.
Personnaliser l'authentification	En fonction de votre scénario de sécurité spécifique, BlackBerry Enterprise Identity vous permet de choisir le mode d'authentification pour chaque service, groupe d'utilisateurs ou les deux. Vous pouvez même adapter les stratégies de votre organisation aux situations à haut risque.
Faire progresser votre stratégie mobile	Les utilisateurs et leurs identités sont essentiels pour la mobilité de l'entreprise. BlackBerry Enterprise Identity unifie et simplifie l'accès aux services en nuage tels que Microsoft Office 365, Salesforce, Google Apps, BlackBerry Workspaces ou la plupart des autres applications et services SAML, afin de prendre en charge la productivité de votre personnel de plus en plus mobile.
Tirer parti de votre solution actuelle de gestion de la mobilité d'entreprise avec BlackBerry	Enterprise Identity est complètement intégré à BlackBerry UEM et offre une gestion de la mobilité d'entreprise de pointe avec un meilleur contrôle de l'accès à tous vos services en nuage. Cela vous permet d'accéder à des fonctionnalités, comme le provisionnement d'applications en un clic et le droit d'identification unique, BlackBerry 2FA et Mobile Zero Sign-On (Mobile ZSO).

Utilisation de Enterprise Identity pour la première fois

BlackBerry UEM et BlackBerry UEM Cloud comprennent le logiciel BlackBerry Enterprise Identity. Dans BlackBerry UEM version 12.7 MR1 et ultérieure, vous n'avez pas besoin d'activer Enterprise Identity. Si votre organisation possède la licence appropriée, Enterprise Identity est automatiquement activé.

Bien comprendre les services, les droits d'utilisateurs et les groupes

Les services sont des applications, souvent en nuage, auxquelles les utilisateurs doivent accéder. Par exemple, Microsoft Office 365, BlackBerry Workspaces ou WebEx. En configurant un service dans BlackBerry UEM, BlackBerry UEM Cloud ou BlackBerry Enterprise Identity, vous configurez une interface sécurisée entre Enterprise Identity et votre instance, ou locataire, de ce service. Après avoir utilisé BlackBerry UEM ou BlackBerry UEM Cloud pour ajouter un service, utilisez la console de gestion BlackBerry UEM pour gérer le service et attribuer des autorisations au service pour les utilisateurs.

La façon la plus efficace d'autoriser des applications pour vos utilisateurs est d'utiliser les groupes d'application. Un groupe d'applications peut contenir à la fois l'autorisation par identification unique (SSO) pour un service et les applications client nécessaires sur les terminaux pour interagir avec le service. Vous pouvez assigner des groupes d'applications à des utilisateurs ou à des groupes d'utilisateurs, afin de donner aux utilisateurs tout ce dont ils ont besoin pour accéder à ce service.

Les groupes d'utilisateurs donnent aux administrateurs la possibilité d'attribuer des droits à un grand nombre d'utilisateurs d'un seul coup plutôt que de devoir gérer ces droits individuellement pour chaque utilisateur ajouté ou supprimé du groupe. Lorsqu'un utilisateur est ajouté au groupe, le droit lui est automatiquement attribué, lui permettant ainsi de se connecter au service depuis n'importe quel appareil à l'aide des mêmes informations d'identification. Si un utilisateur est supprimé du groupe, il perd automatiquement ses droits d'accès à ce service. Les droits d'utilisation de services peuvent également être attribués individuellement à des utilisateurs spécifiques, le cas échéant.

Licences de termes	Description
Service	Les services incluent Workspaces, Box, Workday, WebEx, Salesforce et d'autres, y compris des services personnalisés.
Droit d'utilisation	Une autorisation est une attribution de service générée avec BlackBerry UEM qui indique à Enterprise Identity de fournir un accès par identification unique à un service pour un utilisateur ou groupe donné.
Groupe d'applications	Un groupe d'applications est un ensemble d'applications qui peut inclure l'autorisation d'accès par identification unique ainsi que les binaires associés pour les appareils mobiles.
Utilisateur	Un utilisateur est une personne qui utilise BlackBerry UEM.
Groupe d'utilisateurs	Un groupe d'utilisateurs regroupe plusieurs utilisateurs de BlackBerry UEM.

Gérer des services

Si vous utilisez BlackBerry UEM 12.7 ou une version ultérieure, ou BlackBerry UEM Cloud, la gestion des services de votre organisation s'effectue avec la console de gestion BlackBerry UEM.

Gestion des services dans la console de gestion BlackBerry UEM

Avant que vous puissiez configurer SaaS ou d'autres services dans la console de gestion BlackBerry UEM, votre administrateur système doit ajouter le service en question. Pour plus d'informations, reportez-vous au contenu relatif à l'intégration des services SaaS.

Dès que votre organisation aura acheté les licences appropriées pour BlackBerry Enterprise Identity (pour plus d'informations, consultez le Guide des licences BlackBerry UEM), vous pourrez utiliser la console BlackBerry UEM pour gérer les services et les fonctionnalités de ces services. L'ajout de services requiert la définition des paramètres de sécurité et d'autres paramètres spécifiques à votre organisation.

Après l'ajout d'un service, vous pouvez autoriser les utilisateurs à l'utiliser sur la base d'un seul utilisateur ou par le biais d'un groupe dans la console de gestion BlackBerry UEM. Vous pouvez modifier la configuration de ce service dans la console de gestion BlackBerry UEM.

Afficher la liste des modèles de services dans la console BlackBerry UEM

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity > Services**.
3. Cliquez sur +.

La liste des modèles de services disponibles s'affiche.

Afficher la liste des services personnalisés que vous avez créés dans la console BlackBerry UEM

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity** > **Services**.

La liste des services personnalisés s'affiche.

Créer un service SaaS dans la console BlackBerry UEM

Remarque : si vous voulez créer deux instances du même type de service dans BlackBerry UEM (par exemple, Box), vous devez fournir des ID d'entité de fournisseur de services différents pour chacune des instances.

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity > Services**.
3. Cliquez sur +.
4. Sélectionnez le type de service que vous souhaitez créer (par exemple Box).
5. Sur l'écran **Ajouter un service BlackBerry Enterprise Identity**, saisissez les métadonnées du fournisseur de services. Ces métadonnées sont propres au fournisseur de service et à votre organisation. Notez que seuls s'affichent les champs qui sont associés au modèle de service sélectionné.

Nom	Description
Identification zéro mobile	Sélectionnez cette option si vous voulez activer l'identification zéro mobile.
Nom	Saisissez le nom du fournisseur SaaS.
Description	La description du locataire est facultative.
Logo	Ajoutez un logo à associer au service.
ID d'entité de fournisseur de services	Saisissez l'URL ou le nom unique que vous utilisez pour accéder au service SaaS.
POST URL du service client d'assertions	Saisissez la POST URL fournie par le fournisseur de service.
Prise en charge de la connexion initiée par IdP	Saisissez le type de prise en charge de connexion dont votre entreprise a besoin.
Options de signature	Saisissez votre choix d'assertion.
Certificat de signature IdP	Saisissez le certificat x509 partagé avec le fournisseur de service.
Clé privée de signature IdP	Saisissez la clé x509 pour le certificat de signature correspondant. Conservez-la en lieu sûr.
Certificat de cryptage	Saisissez le certificat de cryptage.
Informations relatives aux services	Certains services nécessitent des informations supplémentaires ou des informations qui diffèrent légèrement de ces descriptions. La plupart du temps, ces informations sont préconfigurées.
Déclarations - Attribut d'identifiant du nom	Sélectionnez l'attribut d'identifiant de votre déclaration.

Nom	Description

Attributs de la déclaration SAML	• Nom - Saisissez un nom pour la déclaration SAML
	• Attribut SAML - Saisissez votre attribut SAML
	• Type de déclaration SAML
	  • Locale : si vous choisissez une déclaration locale, vous devez sélectionner une option dans la liste de valeur d'attribut. Un attribut SAML sera ainsi mappé à un type d'attribut connu de BlackBerry Enterprise Identity comme le nom d'utilisateur.
	  • Statique : si vous choisissez une déclaration statique, vous devez saisir une option dans le champ de valeur d'attribut.
	  • Répertoire : si vous choisissez l'option Répertoire, vous pouvez saisir le nom d'un attribut Active Directory. Les valeurs qui correspondent au texte que vous saisissez sont automatiquement suggérées.
	• Valeur d'attribut - sélectionnez ou tapez une valeur d'attribut. Il s'agit d'une valeur définie dont votre service SaaS pourrait avoir besoin pour configurer le service pour les utilisateurs de votre organisation.
	• Type d'attribut - sélectionnez un type pour l'attribut. Le type est basé sur vos besoins en matière de services SaaS. La valeur par défaut est anyType.
	• Si vous souhaitez que l'attribut soit obligatoire, vous pouvez également cocher la case **Requis**.

6. Cliquez sur **Enregistrer**.

Ajouter un service de fournisseur de revendications AD FS

Si votre organisation dispose d'applications qui utilisent l'authentification basée sur des formulaires des services de fédération Active Directory (AD FS), vous pouvez ajouter un service de fournisseur de revendications AD FS afin de pouvoir vous authentifier auprès des applications AD FS Enterprise Identity à l'aide du type d'authentification par formulaires.

Enterprise Identity prend en charge AD FS 2019 et versions ultérieures

Avant de commencer :

- Vérifiez que le rôle AD FS a été ajouté au serveur Active Directory.
- Vérifiez que UEM est connecté au serveur Active Directory qui a le rôle AD FS.

1. Dans la console de gestion UEM, cliquez sur **Paramètres** > **BlackBerry Enterprise Identity** > **Services**.
2. Dans le tableau **Services SAML**, cliquez sur +.
3. Cliquez sur **Fournisseur de revendications ADFS**.
4. Si vous souhaitez activer ZSO pour les utilisateurs, cochez les cases **Autoriser une connexion Mobile ZSO lorsque la politique d'authentification le précise le précise** et **Autoriser une connexion Kerberos Desktop ZSO lorsque la politique d'authentification le précise**.
5. Saisissez le nom et la description du service.
6. Dans le champ **ID d'entité du fournisseur de services**, saisissez `http://<adfs_host>/adfs/services/trust`, où *adfs_endpoint* est le nom du serveur Active Directory qui a le rôle ADFS.
7. Dans le champ **POST URL du service client d'assertions**, saisissez `http://<adfs_host>/adfs/services/ls`, où *adfs_endpoint* est le nom du serveur Active Directory qui a le rôle ADFS.
8. Dans le champ **URL du service de déconnexion unique**, saisissez `http://<adfs_host>/adfs/services/ls`, où *adfs_endpoint* est le nom du serveur Active Directory qui a le rôle ADFS.

9. Cliquez sur **Enregistrer**.

À la fin : Attribuez le service aux utilisateurs.

Configurer le fournisseur de revendications dans AD FS

Avant de commencer : Ajouter un service de fournisseur de revendications AD FS

1. Dans la console de gestion UEM, cliquez sur **Paramètres** > **BlackBerry Enterprise Identity** > **Services**.
2. Dans le tableau **Services SAML**, cliquez sur le service Fournisseur de revendications AD FS.
3. Dans la section **Métadonnées du service SAML**, cliquez sur le lien pour télécharger les métadonnées du service SAML. Copiez le fichier sur le serveur Windows qui exécute AD FS.
4. Ouvrez le gestionnaire AD FS.
5. Dans le volet de gauche, cliquez sur **Approbations de fournisseur de revendications**.
6. Dans le volet de droite, cliquez sur **Ajouter un fournisseur de revendications**.
7. Dans l'**Assistant Ajout d'approbation de fournisseur de revendications**, cliquez sur **Démarrer** > **Suivant**.
8. Sélectionnez **Importer les données relatives au fournisseur de revendications à partir d'un fichier** et ouvrez le fichier de métadonnées que vous avez téléchargé à l'étape 3. Cliquez sur **Suivant**.
9. Saisissez le nom et la description de l'approbation de fournisseur de revendications. Cliquez sur **Suivant** jusqu'à ce que le bouton Enregistrer s'affiche.
10. Cliquez sur **Enregistrer**.

Si vous souhaitez tester votre configuration ADFS, vous pouvez créer une application test à l'aide de Claims X-Ray. Pour plus d'informations, rendez-vous sur https://adfshelp.microsoft.com/ClaimsXray/TokenRequest

Utiliser Enterprise Identity comme fournisseur de revendications par défaut

Pour utiliser Enterprise Identity comme fournisseur de revendications par défaut, vous pouvez exécuter la commande suivante dans Windows PowerShell. Lorsque Enterprise Identity est le fournisseur de revendications par défaut, les utilisateurs ne sont pas invités à s'authentifier lorsqu'ils accèdent à un service.

Dans Windows PowerShell, exécutez la commande suivante :

```
Set-AdfsRelyingPartyTrust -TargetName <relying_party_name> -ClaimsProviderName
 @("<claims_provider_display_name>")
```

Exemple : Configurer le mappage des revendications pour Office 365

Les étapes suivantes présentent un exemple de configuration d'un mappage de base des revendications pour Microsoft Office 365. Votre organisation peut avoir des exigences différentes en matière de mappage des revendications.

Avant de commencer : Utiliser Enterprise Identity comme fournisseur de revendications par défaut.

1. Dans le gestionnaire AD FS, cliquez sur **Modifier les règles de revendication** pour le fournisseur de revendications Enterprise Identity que vous avez configuré.
2. Cliquez sur **Ajouter une règle** > **Envoyer des revendications à l'aide d'un rôle personnalisé**.
3. Dans la fenêtre de modèle **Sélectionner une règle**, dans la liste déroulante **Modèle de règle de revendication**, sélectionnez **Envoyer des revendications à l'aide d'une règle personnalisée**. Cliquez sur **Suivant**.
4. Dans la fenêtre **Configurer une règle**, dans le champ **Nom de la règle de revendication**, saisissez `Transmettre toutes les revendications`.

5. Dans le volet **Règle personnalisée**, entrez les informations suivantes :

```
c:[]
            => issue(claim = c);
```

6. Cliquez sur **Terminer**.
7. Dans la fenêtre **Configurer une règle**, dans le champ **Nom de la règle de revendication**, saisissez `Transformer l'UPN`.
8. Dans le volet **Règle personnalisée**, entrez les informations suivantes :

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
 => issue(Type = "http://schemas.xmlsoap.org/claims/UPN", Issuer =
 c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = regexreplace(c.Value,
 "^(?<utilisateur>.*)$", "${user}<suffixe_de_domaine_pour_vos_utilisateurs>"),
 ValueType = c.ValueType);
```

   Dans lesquelles le suffixe de domaine est le domaine de messagerie pour les utilisateurs (par exemple « ${utilisateur}@exemple.com »).
9. Cliquez sur **Terminer**.
10. Dans la console de gestion UEM, cliquez sur **Paramètres** > **BlackBerry Enterprise Identity** > **Services**.
11. Dans le tableau **Services SAML**, cliquez sur le service ADFS que vous avez créé.
12. Sous **Revendications**, dans la liste déroulante **Attribut d'identifiant du nom**, sélectionnez **ID immuable**.
13. Dans le tableau des attributs de revendication SAML, cliquez sur +. Procédez comme suit :
    a) Dans le champ Nom, saisissez `Nom d'utilisateur`.
    b) Sous Attribut SAML, sélectionnez http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name.
    c) Définissez le type de revendication SAML sur Local.
    d) Définissez la valeur de l'attribut sur le nom que vous avez saisi pour l'attribut de revendication (par exemple, Nom d'utilisateur).
    e) Définissez la valeur de l'attribut sur anyType.
    f) Cliquez sur **Enregistrer**.
14. Dans le tableau des attributs de revendication SAML, cliquez sur +. Procédez comme suit :
    a) Dans le champ Nom, saisissez `UPN`.
    b) Sous Attribut SAML, sélectionnez http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn.
    c) Définissez le type de revendication SAML sur Local.
    d) Définissez la valeur de l'attribut sur le nom que vous avez saisi pour l'attribut de revendication (par exemple, UPN).
    e) Définissez la valeur de l'attribut sur anyType.
    f) Cliquez sur **Enregistrer**.
15. Dans le tableau des attributs de revendication SAML, cliquez sur +. Procédez comme suit :
    a) Dans le champ Nom, saisissez `ID immuable`.
    b) Sous Attribut SAML, sélectionnez http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID.
    c) Définissez le type de revendication SAML sur Local.
    d) Définissez la valeur de l'attribut sur le nom que vous avez saisi pour l'attribut de revendication (par exemple, ID immuable).
    e) Définissez la valeur de l'attribut sur anyType.
16. Cliquez sur **Enregistrer**.

Ajouter un service personnalisé dans la console BlackBerry UEM

BlackBerry fournit une gamme croissante de modèles de services prédéfinis. En tant qu'administrateur, vous pouvez également ajouter des services personnalisés à BlackBerry Enterprise Identity. La plupart des services qui utilisent les protocoles SAML 2.0 peuvent être intégrés. Les services SAML que vous intégrez peuvent être personnalisés et spécifiques à votre organisation. Vous pouvez également choisir d'intégrer un service d'un fournisseur SaaS plus largement utilisé.

Lorsqu'un service est activé, les utilisateurs auxquels vous attribuez des droits pourront l'utiliser. Lorsqu'un service est désactivé, tous les utilisateurs ayant des droits sur ce service les perdront jusqu'à ce qu'il soit réactivé.

Pour des informations détaillées sur les modèles de services disponibles, reportez-vous à la section Intégration de services SaaS.

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity > Services**.
3. Cliquez sur +.
4. Sélectionnez **Service personnalisé**.
5. Remplissez les champs pour configurer le service personnalisé.
   - Lorsque vous ajoutez une demande SAML, si vous choisissez une demande locale, vous devez ensuite sélectionner une option dans la liste de valeur d'attribut. Cela reliera un attribut SAML à un type d'attribut connu de BlackBerry Enterprise Identity comme le nom d'utilisateur.
   - Lorsque vous ajoutez une demande SAML, si vous choisissez une demande statique, vous devez saisir une option dans le champ de valeur d'attribut.
6. Cliquez sur **Enregistrer**.

Modifier un service activé dans la console BlackBerry UEM

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity > Services**.
3. Cliquez sur le service que vous souhaitez modifier.
4. Pour modifier la configuration de service d'un service ou d'une fonctionnalité modifiable, remplissez les champs dans la section **Configuration de service**. Certains services peuvent ne pas autoriser les modifications.
5. Cliquez sur **Enregistrer**.

Supprimer un service dans la console BlackBerry UEM

Avant de supprimer un service, vous devez supprimer tous les droits attribués aux utilisateurs pour ce service dans la console de gestion BlackBerry UEM.

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity > Services**.
3. Cliquez sur X en regard du service que vous souhaitez supprimer.
4. Cliquez sur **Supprimer.**

Afficher les paramètres de configuration SAML dans la console BlackBerry UEM

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity > Services**.
3. Cliquez sur la configuration de services SaaS pour afficher les paramètres SAML.

Exporter les métadonnées du service SAML dans la console BlackBerry UEM

Il est possible que vous ayez besoin des métadonnées du service SAML pour configurer l'interface sécurisée entre BlackBerry Enterprise Identity et votre instance du service, ou le locataire du service, que vous êtes en train de configurer (par exemple, Box).

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity > Services**.
3. Cliquez sur la configuration de services SaaS pour afficher l'en-tête des métadonnées SAML.
4. Cliquez sur le lien hypertexte pour télécharger le fichier XML.

Ajouter une application OpenID Connect

Vous pouvez ajouter des applications OpenID Connect qui ont été mises à la disposition de votre organisation ou de votre locataire UEM. Les applications OpenID Connect sont mises à disposition par un administrateur ou le développeur d'applications.

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menus.
2. Cliquez sur **BlackBerry Enterprise Identity** > **Services**.
3. Dans le tableau des **applications OpenID Connect**, cliquez sur +.
   Une liste des applications OpenID Connect disponibles s'affiche.
4. Sélectionnez une application.
5. Sur l'écran **Ajouter un service BlackBerry Enterprise Identity**, effectuez l'une des actions suivantes :
   - Sélectionnez l'option **Autoriser une connexion Mobile ZSO lorsque la politique d'authentification le précise**
   - Sélectionnez l'option **Autoriser une connexion Kerberos Desktop ZSO lorsque la politique d'authentification le précise**
6. Examinez les étendues de l'application. Cliquez sur **Enregistrer**.

Pour modifier l'application, cliquez sur le nom de l'application dans le tableau des applications OpenID Connect.

Mettre à jour le consentement pour une application OpenID Connect

Si les étendues requises pour une modification d'application OpenID Connect sont modifiées, vous devez mettre à jour le consentement pour l'application. Lorsque les étendues requises sont modifiées, une notification s'affiche dans la section OpenID Connect de la page Services de BlackBerry Enterprise Identity.

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menus.
2. Cliquez sur **BlackBerry Enterprise Identity** > **Services**.
3. Dans le tableau des applications **OpenID Connect**, cliquez sur la notification d'une application dans la section **Consentement obligatoire**.
4. Dans la boîte de dialogue **Mettre à jour l'application**, examinez les étendues ou les clients qui ont été ajoutés ou supprimés. Cliquez sur **Enregistrer**.

Supprimer une application OpenID Connect

1. Sur la console de gestion de BlackBerry UEM, cliquez sur **Paramètres** dans la barre de menu.
2. Cliquez sur **BlackBerry Enterprise Identity** > **Services**.
3. Dans le tableau **Applications OpenID Connect**, cliquez sur ✕ en regard de l'application que vous souhaitez supprimer.
4. Dans la boite de dialogue **Retirer le consentement**, cliquez sur **Supprimer**.

Connexion à la console BlackBerry Enterprise Identity

Vous aurez peut-être besoin de vous connecter à la console BlackBerry Enterprise Identity pour effectuer certaines tâches telles qu'afficher les journaux du système.

Avant de commencer : activez les fenêtres contextuelles dans votre navigateur.

1. Sur la console de gestion BlackBerry UEM, dans la barre de menu, cliquez sur **Applications**.
2. Cliquez sur **Enterprise Identity**. Un message vous demandant de synchroniser les services Enterprise Identity s'affiche.
3. Cliquez sur **Ouvrir la console Enterprise Identity**. La console d'administration s'ouvre dans un nouvel onglet de navigateur. Si la console ne s'ouvre pas, vérifiez que vous avez activé les fenêtres contextuelles dans votre navigateur.
4. Une fois terminé, fermez l'onglet du navigateur.

Gestion des niveaux d'authentification

Trois types d'authentification sont disponibles dans Enterprise Identity. La classification de ces authentificateurs peut être modifiée dans la console BlackBerry UEM, sur la page **Paramètres**. Pour plus d'informations sur la classification, reportez-vous à la section Modification des paramètres Enterprise Identity.

Type d'authentificateur	Description
Mot de passe d'entreprise	Cette méthode de sécurité nécessite un mot de passe pour que les utilisateurs puissent accéder à un service. Il s'agit de la méthode par défaut. Le mot de passe est un mot de passe associé actuellement à un compte utilisateur dans Active Directory, un annuaire LDAP ou BlackBerry UEM.
Mot de passe d'entreprise et BlackBerry 2FA	Cette méthode de sécurité tire parti de BlackBerry 2FA et nécessite à la fois un mot de passe et un accusé de réception sur le terminal mobile d'un utilisateur avant que celui-ci puisse accéder à un service.
Mobile ZSO	Cette méthode de sécurité, disponible sur les terminaux mobiles, permet à un utilisateur d'accéder à un service sans devoir s'authentifier explicitement. Au lieu de cela, il utilise l'authentification de l'utilisateur avec le terminal ou le conteneur sécurisé comme preuve d'identité.
Mot de passe Ping	Cette méthode de sécurité, accessible aux utilisateurs de PingFederate , exige que les utilisateurs saisissent leur mot de passe Ping Identity avant de pouvoir accéder à un service. Pour plus de sécurité, vous pouvez également demander aux utilisateurs d'accuser réception d'une invite ou de saisir leur PingID.

Vous pouvez attribuer ces niveaux d'authentification à l'utilisateur ou au groupe pour chaque service en définissant une stratégie d'authentification. Pour plus d'informations sur les stratégies, consultez Gestion des stratégies d'authentification.

Activer l'authentification à deux facteurs

L'activation de l'authentification à deux facteurs signifie l'activation de BlackBerry 2FA, l'attribution de sa classification d'authentification et d'une stratégie d'authentification qui exige son niveau d'authentification.

Avant de commencer :

- Activez BlackBerry 2FA dans BlackBerry UEM et appliquez le profil BlackBerry 2FA à l'utilisateur ou au groupe.
- Assurez-vous que tous les utilisateurs qui doivent utiliser BlackBerry 2FA disposent d'un terminal mobile et que celui-ci est activé. Pour plus d'informations sur l'activation des terminaux, consultez le contenu relatif à BlackBerry 2FA.

1. Attribuez un niveau d'authentification à BlackBerry 2FA. Pour plus d'informations, reportez-vous à la section Gestion des niveaux d'authentification.
2. Configurez une stratégie d'authentification qui spécifie BlackBerry 2FA en tant que niveau d'authentification à utiliser par un groupe d'utilisateurs spécifique ou un service spécifique. Pour plus d'informations, reportez-vous à la section Gestion des stratégies d'authentification.

Activation de Mobile ZSO

Lorsque vous activez l'identification Mobile Zero Sign-On (Mobile ZSO), vous l'activez pour les services que vous souhaitez utiliser, vous décidez de son classement d'authentification et vous attribuez une stratégie d'authentification qui requiert son niveau d'authentification.

L'activation de Mobile ZSO pour un service permet à ce dernier de s'authentifier avec un certificat sur le terminal géré d'un utilisateur sans devoir utiliser de nom d'utilisateur ni de mot de passe.

Activation de Mobile ZSO dans BlackBerry UEM

Avant de commencer :

- Les utilisateurs doivent posséder un terminal Android Enterprise activé avec un profil de travail, un terminal Samsung Knox, iOS ou BlackBerry 10.
- Les utilisateurs doivent disposer de BlackBerry Secure Connect Plus sur leurs terminaux.

1. Connectez-vous à BlackBerry UEM en tant qu'administrateur.
2. Dans la barre de menus, cliquez sur **Paramètres > BlackBerry Enterprise Identity > Services**.
3. Cliquez sur le service pour lequel vous souhaitez activer Mobile ZSO.
4. Sélectionnez l'option **Autoriser Mobile ZSO lorsqu'il est spécifié par la stratégie d'authentification**.
5. Cliquez sur **Enregistrer**.
6. Attribuez Mobile ZSO à un niveau d'authentification. Pour plus d'informations, reportez-vous à la section Gestion des niveaux d'authentification.
7. Configurez une stratégie d'authentification qui spécifie Mobile ZSO en tant que niveau d'authentification à utiliser par un groupe d'utilisateurs ou un service spécifique. Pour plus d'informations, reportez-vous à la section Gestion des stratégies d'authentification.

L'activation de Mobile Zero Sign-On (Mobile ZSO) pour un service autorise ce dernier à s'authentifier à l'aide de Mobile ZSO. La stratégie d'authentification globale attribuée dans BlackBerry UEM doit accorder une autorisation à Mobile ZSO.

Si vous configurez un service pour Mobile ZSO sans authentificateur de secours, il sera accessible uniquement à partir de terminaux mobiles gérés. Toutefois, si un authentificateur de secours est configuré, Mobile ZSO sera utilisé sur les terminaux mobiles gérés et l'utilisateur sera autorisé à utiliser le mot de passe sur d'autres terminaux.

Gestion des facteurs de risque

Les facteurs de risque sont des fonctionnalités facultatives des stratégies d'authentification qui permettent d'équilibrer le niveau d'authentification en fonction du risque. Lorsqu'un utilisateur se trouve dans un navigateur ou réseau sécurisé, il peut accéder plus facilement aux services dont il a besoin ; vous pouvez cela dit appliquer une stratégie d'authentification plus stricte dans d'autres circonstances.

Facteurs de risque	Description
Détection du navigateur	Ce facteur de risque demande aux utilisateurs d'établir une référence d'approbation entre le navigateur et Enterprise Identity lors de leur première ouverture d'un navigateur. Une fois l'approbation établie, les connexions suivantes peuvent utiliser un niveau d'authentification plus simple. Les utilisateurs peuvent afficher et supprimer les entrées de navigateur approuvées dans BlackBerry UEM Self-Service.
Détection du réseau	Ce facteur de risque détermine si l'application ou le navigateur d'un utilisateur est connecté(e) au même réseau que le serveur BlackBerry UEM. Si ce n'est pas le cas, un niveau d'authentification plus élevé peut être appliqué. Ce facteur de risque peut permettre aux utilisateurs de se connecter plus facilement à certains services lorsqu'ils se trouvent sur leur réseau professionnel. Pour plus d'informations sur la configuration de ce facteur de risque, consultez Configurer le facteur de risque de détection du réseau. Si vous voulez désactiver globalement la détection du réseau, vous pouvez vous connecter à la console Enterprise Identity et désactiver Détection du réseau professionnel dans la liste des locataires UEM. **Remarque :** Il n'est pas possible d'activer le facteur de risque de détection de réseau dans BlackBerry UEM Cloud.

Configurer le facteur de risque de détection du réseau

Avant de commencer : Il n'est pas possible d'activer le facteur de risque de détection de réseau dans BlackBerry UEM Cloud.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > BlackBerry Enterprise Identity > Paramètres**.
2. Saisissez le nom d'hôte du réseau professionnel du serveur BlackBerry UEM qu'utilisent vos ordinateurs et terminaux professionnels. Si vous préférez, vous pouvez également saisir le nom de pool DNS qui couvre plusieurs adresses IP du serveur BlackBerry UEM.
3. Confirmez que vos ordinateurs et terminaux professionnels peuvent se connecter au nom d'hôte à l'aide du numéro de port répertorié. Le facteur de risque ne fonctionne pas si le port est bloqué par un pare-feu.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **Paramètres** > **Infrastructure** > **Certificats de serveur** > **Certificat SSL pour BlackBerry Web Services**.

   Les terminaux et les navigateurs d'ordinateur professionnel doivent approuver le certificat lorsqu'ils se connectent au nom d'hôte du réseau professionnel. Le certificat par défaut est alors auto-signé et non approuvé. Vous pouvez télécharger un certificat BlackBerry Web Services approuvé dans BlackBerry UEM.

À la fin : Certains navigateurs Web peuvent exiger un certificat approuvé en externe. Si c'est le cas, un nouveau certificat BlackBerry Web Services peut être chargé dans BlackBerry UEM. Cliquez sur **Paramètres** > **Infrastructure** > **Certificats de serveur** > **Certificat SSL pour BlackBerry Web Services**.

À la fin : Lorsque vous créez ou modifiez une stratégie d'authentification Enterprise Identity, cochez la case **Détection du réseau** pour ajouter le facteur de risque. Pour plus d'informations sur la création de stratégies d'authentification, consultez Créer une stratégie d'authentification Enterprise Identity.

Gestion des stratégies d'authentification

Vous pouvez utiliser la console de gestion BlackBerry UEM pour créer, gérer et classer les stratégies d'authentification. Les stratégies peuvent être remplacées pour chaque service. Pour obtenir des informations générales sur les stratégies et profils, reportez-vous à la section Stratégies informatiques dans le contenu relatif à l'administration de BlackBerry UEM.

Créer une stratégie d'authentification Enterprise Identity

Effectuez l'opération suivante pour créer une stratégie Enterprise Identity pour des groupes d'utilisateurs.

1. Sur la barre de menus de la console de gestion BlackBerry UEM, cliquez sur **Stratégies et profils** > **BlackBerry Enterprise Identity**.
2. Cliquez sur + en regard des **Stratégies d'authentification**.
3. Saisissez le nom et la description du profil.
4. Dans la liste déroulante **Niveau minimal d'authentification**, spécifiez un niveau d'authentification. Pour plus d'informations, reportez-vous à la section Gestion des niveaux d'authentification.
5. Dans le tableau **Scénario de risque**, cliquez sur +.
6. Saisissez un nom et une description.
7. Dans la liste déroulante **Niveau minimal d'authentification**, sélectionnez le niveau d'authentification souhaité lorsque les facteurs de risque correspondent.
8. Dans la liste **Combinaison de facteur de risque**, choisissez l'une des options suivantes :
   - Si vous voulez appliquer tous les facteurs de risque au scénario, sélectionnez **Tous les facteurs sélectionnés sont présents**
   - Si vous souhaitez appliquer l'un des facteurs de risque sélectionnés au scénario, sélectionnez **L'un des facteurs sélectionnés est présent**
9. Si vous voulez évaluer si une application d'utilisateur ou le navigateur est connecté au même réseau que le serveur BlackBerry UEM, sélectionnez l'option **Détection de réseau**, puis sélectionnez l'option souhaitée dans la liste déroulante **Configuration**. Notez qu'il n'est pas possible d'activer le facteur de risque de détection de réseau dans BlackBerry UEM Cloud.
10. Si vous voulez établir une référence d'approbation entre le navigateur et Enterprise Identity la première fois qu'un utilisateur ouvre un navigateur, sélectionnez l'option **Détection du navigateur**, puis sélectionnez l'option souhaitée dans la liste déroulante **Configuration**.
11. Si vous souhaitez utiliser les zones géographiques et les niveaux de risque de BlackBerry Persona Mobile comme facteurs de risque, choisissez l'option **BlackBerry Persona** et sélectionnez l'une des options suivantes :
    - **Niveau de risque comportemental** : les services cloud BlackBerry Persona de BlackBerry Infrastructure collectent et traitent des données d'application et les utilisent pour calculer un niveau de risque pour chaque utilisateur.
    - **Zone géographique définie par l'administrateur** : choisissez une zone géographique créée par l'administrateur BlackBerry UEM de votre organisation.

      Remarque : Pour plus d'informations sur les niveaux de risque et les zones géographiques, reportez-vous au contenu relatif à BlackBerry Persona Mobile.
    - **Niveau de risque de la zone géographique** : choisissez entre Élevé, Moyen ou Faible. Ce paramètre spécifie un niveau de risque qui peut être attribué à un utilisateur en comparant l'emplacement physique de l'utilisateur à la région contenue dans une zone géographique apprise ou définie par l'administrateur.
12. Cliquez sur **Enregistrer**.

13. Si vous voulez créer une exception pour les services de votre organisation, cliquez sur **Gérer les exceptions de service**, sélectionnez le service dans la liste, et définissez les scénarios de risque nécessaires pour ce service.
14. Si nécessaire, répétez les étapes 5 à 11 pour ajouter des scénarios de risque supplémentaires. Notez que chaque scénario de risque doit utiliser un ensemble unique de facteurs de risque.
15. Cliquez sur **Enregistrer**.

Attribuer une stratégie Enterprise Identity à un groupe d'utilisateurs

Avant de commencer : Créez une stratégie Enterprise Identity.

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Groupes** > **Utilisateurs** sur la barre de menu.
2. Créez un nouveau groupe ou cliquez sur le nom du groupe que vous voulez modifier.
3. Cliquez sur l'onglet **BlackBerry Enterprise Identity**.
4. Cliquez sur +.
5. Choisissez une stratégie d'authentification dans la liste déroulante.
6. Cliquez sur **Attribuer**.

Supprimer une stratégie Enterprise Identity

Avant de commencer : Créez un profil Enterprise Identity.

1. Sur la barre de menus de la console de gestion BlackBerry UEM, cliquez sur **Stratégies et profils** > **BlackBerry Enterprise Identity**.
2. Cliquez sur le nom du profil que vous souhaitez supprimer.
3. Cliquez sur  .
4. Cliquez sur **OK**.

Utilisation de la classification du niveau d'authentification des stratégies d'authentification pour gérer la sécurité

Vous pouvez utiliser la classification du niveau d'authentification et les stratégies d'authentification BlackBerry Enterprise Identity pour spécifier les types d'authentification que les utilisateurs doivent réaliser lors de la connexion à un service. Les classifications d'authentificateurs sont des méthodes de sécurité qui définissent le type d'authentification de l'utilisateur requis lors de la connexion au service. Utilisez des scénarios de risque et les facteurs de risque dans le cadre d'une stratégie d'authentification pour spécifier les paramètres qui s'appliquent aux utilisateurs et aux groupes lorsqu'ils accèdent aux services Enterprise Identity.

Nécessité d'une authentification supplémentaire lorsque les utilisateurs sont connectés à un réseau externe

Pour demander aux utilisateurs de saisir leur mot de passe et de répondre à une invite BlackBerry 2FA lorsque les utilisateurs essayent de se connecter à un service à l'aide d'un réseau externe, procédez comme suit. Vous pouvez également permettre aux utilisateurs de s'authentifier en utilisant uniquement leur mot de passe à partir de n'importe quel réseau. **Remarque :** il n'est pas possible d'activer le facteur de risque de détection de réseau dans BlackBerry UEM Cloud.

Définir le classement des authentificateurs

1. Dans la barre de menus, cliquez sur **Paramètres > BlackBerry Enterprise Identity > Paramètres**.
2. Dans la section **Classification du niveau d'authentification**, définissez **Mot de passe d'entreprise** au Niveau 1 et **Mot de passe d'entreprise + BlackBerry 2FA** au Niveau 3. Pour plus d'informations sur la configuration de BlackBerry 2FA, voir Activer l'authentification à deux facteurs.
3. Cliquez sur **Enregistrer**.

Ajout d'une stratégie d'authentification pour les réseaux externes

1. Sur la barre de menus, cliquez sur **Stratégies et profils**. Cliquez sur **BlackBerry Enterprise Identity** en dessous de Terminaux gérés.
2. Dans le volet **Stratégies d'authentification**, cliquez sur **Ajouter une stratégie**.
3. Saisissez le nom et la description de la stratégie d'authentification.
4. Dans la liste déroulante **Niveau minimal d'authentification**, sélectionnez Niveau 1.

   Ce niveau correspond à la classification d'authentificateur Enterprise password que vous avez définie dans la tâche précédente. Si vous enregistrez cette stratégie sans ajouter un scénario de risque et l'attribuez à des utilisateurs, ils devront saisir leur mot de passe d'entreprise lorsqu'ils se connecteront à un service. Si vous voulez demander une authentification supplémentaire en fonction du type de réseau auquel les utilisateurs sont connectés, procédez comme suit pour ajouter un scénario de risque.
5. Dans le tableau **Scénario de risque**, cliquez sur +.
6. Saisissez le nom et la description du scénario.
7. Dans la liste déroulante **Niveau minimal d'authentification**, sélectionnez Niveau 3. Ce niveau correspond à la classification d'authentificateur Enterprise password + BlackBerry 2FA que vous avez définie dans la tâche précédente.
8. Cliquez sur **Détection de réseau**.

9. Dans la liste déroulante **Configuration** , sélectionnez **Pas sur un réseau professionnel**.

   Si vous configurez cette option, lorsqu'un utilisateur de votre organisation n'est pas sur un réseau professionnel et qu'il essaye de se connecter à un service, il doit saisir son mot de passe d'entreprise et répondre à une invite BlackBerry 2FA sur son terminal.
10. Cliquez sur **Enregistrer**.
11. Cliquez sur **Enregistrer**.

À la fin :

- Attribuez la stratégie d'authentification à des utilisateurs ou à des groupes.

Demander une authentification supplémentaire lorsque les utilisateurs utilisent un navigateur pour la première fois

Effectuez les tâches suivantes pour demander aux utilisateurs de saisir leur mot de passe et de répondre à une invite BlackBerry 2FA lorsqu'ils essayent de se connecter à un service à l'aide d'un navigateur pour la première fois. Une fois l'approbation établie, les connexions suivantes peuvent utiliser un niveau d'authentification plus simple.

Définir le classement des authentificateurs

1. Dans la barre de menus, cliquez sur **Paramètres > BlackBerry Enterprise Identity > Paramètres**.
2. Dans la section **Classification du niveau d'authentification**, définissez **Mot de passe d'entreprise** au Niveau 1 et **Mot de passe d'entreprise + BlackBerry 2FA** au Niveau 3. Pour plus d'informations sur la configuration de BlackBerry 2FA, voir Activer l'authentification à deux facteurs.
3. Cliquez sur **Enregistrer**.

Ajout d'une stratégie d'authentification pour la première utilisation d'un navigateur

1. Sur la barre de menus, cliquez sur **Stratégies et profils**. Cliquez sur **BlackBerry Enterprise Identity** en dessous de Terminaux gérés.
2. Dans le volet **Stratégies d'authentification**, cliquez sur **Ajouter une stratégie**.
3. Saisissez le nom et la description de la stratégie d'authentification.
4. Dans la liste déroulante **Niveau minimal d'authentification**, sélectionnez Niveau 1.

   Ce niveau correspond à la classification d'authentificateur Enterprise password que vous avez définie dans la tâche précédente. Si vous enregistrez cette stratégie sans ajouter un scénario de risque et l'attribuez à des utilisateurs, ils devront saisir leur mot de passe d'entreprise lorsqu'ils se connecteront à un service. Si vous voulez demander une authentification supplémentaire si les utilisateurs utilisent le navigateur pour la première fois, procédez comme suit pour ajouter un scénario de risque.
5. Dans le tableau **Scénario de risque**, cliquez sur +.
6. Saisissez le nom et la description du scénario.
7. Dans la liste déroulante **Niveau minimal d'authentification**, sélectionnez Niveau 3. Ce niveau correspond à la classification d'authentificateur Enterprise password + BlackBerry 2FA que vous avez définie dans la tâche précédente.
8. Cliquez sur **Détection de réseau**.
9. Dans la liste déroulante **Configuration**, sélectionnez **Navigateur détecté pour la première fois**.

   Si vous configurez cette option, lorsqu'un utilisateur de votre organisation utilise un navigateur pour la première fois et qu'il essaye de se connecter à un service, il doit saisir son mot de passe d'entreprise et répondre à une invite BlackBerry 2FA sur son terminal.

10. Cliquez sur **Enregistrer**.
11. Cliquez sur **Enregistrer**.

À la fin :

- Attribuez la stratégie d'authentification à des utilisateurs ou à des groupes.

Permettre aux utilisateurs de s'authentifier avec PingFederate

BlackBerry Enterprise Identity peut rediriger l'authentification de l'utilisateur vers PingFederate, qui fournit aux utilisateurs Ping Identity existants une interface utilisateur familière. Vous pouvez également utiliser des stratégies BlackBerry Enterprise Identity ou BlackBerry Intelligent Security pour permettre à l'authentification de Ping Identity de s'adapter à la fois au risque et au contexte, y compris l'extension par PingID ou l'authentification multifactorielle BlackBerry 2FA.

Avant que BlackBerry Enterprise Identity et PingFederate puissent communiquer, vous devez créer un client Ping Identity sur le serveur PingFederate de votre organisation, ainsi qu'un fournisseur d'identité correspondant dans BlackBerry UEM.

Avant de créer un client Ping Identity, assurez-vous que l'attribut OBJECTGUID de la stratégie d'authentification PingFederate de votre organisation est défini sur Hex. Pour plus d'informations, consultez la documentation relative à Ping Identity.

Remarque : La dernière version de BlackBerry UEM 12.11 doit être installée dans votre environnement.

Créer un client Ping Identity sur un serveur PingFederate

Avant que vos utilisateurs BlackBerry Enterprise Identity puissent s'authentifier avec PingFederate, vous devez configurer un client Ping Identity sur le serveur PingFederate de votre entreprise.

1. Connectez-vous à la console d'administration PingFederate.
2. Cliquez sur **Serveur OAuth**.
3. Sous la colonne Clients, cliquez sur **Créer nouveau**.
4. Dans le champ **ID client**, saisissez un ID unique pour le client. Notez que vous utiliserez le même ID lorsque vous configurerez le Fournisseur d'identité dans BlackBerry UEM.
5. Saisissez le nom et la description du client.
6. Dans la section Authentification du client, cliquez sur **Clé privée JWT**.
7. Sélectionnez l'option **Exiger des requêtes signées**.
8. Pour générer un jeu de clés Web JSON, rendez-vous sur https://mkjwk.org/.
9. Cliquez sur l'onglet **Courbe elliptique**.
10. Dans la liste déroulante **Courbe**, sélectionnez **P-256**.
11. Dans la liste déroulante **Algorithme**, sélectionnez **ES256**.
12. Cliquez sur **Nouvelle clé**.
13. Copiez la clé à partir du champ **Jeu de paires de clés**. Notez que vous utiliserez cette même clé dans la tâche Configurer un Fournisseur d'identité dans BlackBerry UEM.
14. Collez la clé dans le champ **JWKS** du site PingFederate.
15. Dans le champ **URI de redirection**, ajoutez l'URI du serveur PingFederate de votre entreprise et cliquez sur **Ajouter**.
16. Dans la section **Autorisations accordées**, sélectionnez l'option **Code d'autorisation**.
17. Dans la liste déroulante **Algorithme de signature du jeton ID**, sélectionnez l'une des options **ECDSA**. Notez que vous utiliserez même option dans la tâche Configurer un fournisseur d'identité dans BlackBerry UEM.

18. Cliquez sur **Enregistrer**.

À la fin : Configurer un fournisseur d'identité dans BlackBerry UEM

Configurer un fournisseur d'identité dans BlackBerry UEM

Après avoir créé un client Ping Identity, vous devez créer un fournisseur d'identité correspondant dans la console de gestion BlackBerry UEM.

Avant de commencer : Créer un client Ping Identity sur un serveur PingFederate

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > BlackBerry Enterprise Identity > Fournisseurs d'identité**.
2. Cliquez sur **+** et sélectionnez **PingFederate**.
3. Dans le champ **Nom**, saisissez un nom pour le fournisseur d'identité.
4. Dans le champ **URL du document découverte OIDC**, entrez l'emplacement du serveur PingFederate de votre organisation.
5. Dans le champ **ID Client**, entrez l'ID que vous avez utilisé à l'étape Créer un client Ping Identity sur un serveur PingFederate.
6. Dans le champ **Clé privée JWKS**, entrez la clé que vous avez utilisée à l'étape Créer un client Ping Identity sur un serveur PingFederate.
7. Dans la liste déroulante **Algorithme de signature du jeton d'identité**, sélectionnez l'option que vous avez choisie à l'étape Créer un client Ping Identity sur un serveur PingFederate.
8. Dans la liste **Services disponibles**, sélectionnez les services que vous souhaitez attribuer au client Ping Identity, puis cliquez sur la flèche droite pour déplacer le service dans la liste **Service sélectionné**. Notez que vous ne pouvez attribuer qu'un seul client Ping Identity pour chaque service.
9. Cliquez sur **Enregistrer**.

Créer une stratégie BlackBerry Enterprise Identity pour les utilisateurs PingFederate

1. Dans la barre de menus de la console BlackBerry UEM, cliquez sur **Stratégies et profils > BlackBerry Enterprise Identity > Ajouter une stratégie**.
2. Saisissez le nom et la description de la stratégie.
3. Dans la liste déroulante **Niveau minimal d'authentification**, sélectionnez le numéro correspondant au niveau d'authentification pour l'un des niveaux d'authentification pour Ping Identity sur l'écran **Paramètres > BlackBerry Enterprise Identity > Paramètres**. Vous pouvez choisir un niveau correspondant aux options suivantes : Mot de passe Ping, Mot de passe Ping + BlackBerry 2FA ou Mot de passe Ping + PingID.
4. Si vous le souhaitez, vous pouvez ajouter un Scénario de risque qui fournit une sécurité supplémentaire si certaines conditions sont remplies, par exemple si un utilisateur n'est pas sur un réseau interne. Dans le tableau **Scénario de risque**, cliquez sur **+**.
5. Saisissez le nomet la description du scénario de risque.
6. Sélectionnez un Niveau d'authentification minimum qui correspond à l'un des niveaux d'authentification pour Ping sur l'écran Paramètres > BlackBerry Enterprise Identity > Paramètres. Vous pouvez choisir de permettre à vos utilisateurs de saisir uniquement leur mot de passe, de répondre à une invite BlackBerry 2FA ou de saisir leur PingID si l'un des facteurs de risque est présent lorsque l'utilisateur se connecte au service. Choisissez parmi les Facteurs de risque suivants :

   - **Détection du réseau** : si vous voulez évaluer si l'application ou le navigateur d'un utilisateur est connecté au même réseau que BlackBerry UEM, sélectionnez l'option Détection de réseau, puis l'option souhaitée dans la liste déroulante Configuration.
   - **Détection du navigateur** : si vous voulez établir une référence d'approbation entre le navigateur et Enterprise Identity la première fois qu'un utilisateur ouvre un navigateur, sélectionnez l'option Détection du navigateur, puis l'option souhaitée dans la liste déroulante Configuration.

- **BlackBerry Persona** : si vous voulez utiliser les niveaux de risque et les zones géographiques de BlackBerry Persona Mobile comme facteurs de risque, choisissez l'option BlackBerry Persona

7. Cliquez sur **Enregistrer**.
8. Cliquez sur **Enregistrer**.

À la fin : Attribuez la stratégie aux utilisateurs PingFederate de votre organisation. Si vous avez configuré vos utilisateurs dans un groupe, vous pouvez suivre le sujet Attribuer une stratégie Enterprise Identity à un groupe d'utilisateurs pour affecter facilement la stratégie à tous les utilisateurs à la fois.

Permettre aux utilisateurs de s'authentifier avec Okta

BlackBerry Enterprise Identity peut rediriger l'authentification de l'utilisateur vers Okta, qui fournit une interface utilisateur familière aux utilisateurs Okta existants. Vous pouvez également utiliser les stratégies BlackBerry Enterprise Identity ou BlackBerry Persona pour permettre à l'authentification de Okta de s'adapter à la fois aux risques et au contexte, y compris l'authentification multifacteur BlackBerry 2FA .

Avant que BlackBerry Enterprise Identity et PingFederate puissent communiquer, vous devez créer un client Ping Identity sur le serveur PingFederate de votre organisation, et un fournisseur d'identité correspondant dans BlackBerry UEM.

Avant de créer un client Ping Identity, assurez-vous que l'attribut OBJECTGUID de la stratégie d'authentification PingFederate de votre organisation est défini sur Hex. Pour plus d'informations, consultez la documentation de Ping Identity.

Remarque : La dernière version de BlackBerry UEM 12.11 doit être installée dans votre environnement.

Créer une application Okta

Avant de commencer :

Votre instance Okta doit avoir une connexion à Microsoft Active Directory, et vos utilisateurs doivent être importés dans Okta. Pour obtenir des instructions, reportez-vous à https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-main.htm

1. Connectez-vous à la console d'administration Okta.
2. Créez un jeton de sécurité.
   a) Cliquez sur **Sécurité** > **API** > **Jetons**.
   b) Cliquez sur **Créer un jeton**.
   c) Copiez le jeton.
3. Générez des clés JWKS.
   a) Rendez-vous sur https://mkjwk.org.
   b) Cliquez sur l'onglet **EC**.
   c) Dans la liste déroulante **Courbe**, sélectionnez **P-521**.
   d) Dans la liste déroulante **Algorithme**, sélectionnez **ES521 : ECDSA via P-521 et SHA-512**.
   e) Dans la liste déroulante **ID de clé**, sélectionnez **SHA-256**.
   f) Copiez la paire de clés publique et privée, le jeu de paires de clés et la clé publique.

   Remarque : Dans le jeu de paires de clés publiques et privées, vous devez supprimer l'attribut **"d":**, car il s'agit d'une clé privée.
4. Dans une invite de commande, utilisez une requête CURL/postman pour enregistrer une application OIDC auprès de Okta et mettre à jour les champs suivants dans JSON. La création de ce type d'application n'est actuellement pas prise en charge dans la console Okta.

- Vérifiez que la valeur de l'autorisation SSWS est le jeton que vous avez créé à l'étape 2.
- Remplacez les clés jwks par les clés de l'étape 3.
- Vérifiez que l'attribut "d:" a été supprimé.

Votre saisie doit être similaire à celle-ci :

```
curl --request POST 'https://<oktaDomain>.okta.com/api/v1/apps/' \
--header 'Authorization: SSWS <token>' \
--header 'Content-Type: application/json' \
--data-raw '{
    "name": "oidc_client",
    "label": "BlackBerry Enterprise ID Client",
    "signOnMode": "OPENID_CONNECT",
    "credentials": {
        "oauthClient": {
            "token_endpoint_auth_method": "private_key_jwt"
        }
    },
    "settings": {
        "oauthClient": {
            "redirect_uris": [
                "https://idp.blackberry.com/idp/externalIdpCb"
            ],
            "response_types": [
                "code"
            ],
            "grant_types": [
                "authorization_code"
            ],
            "application_type": "native",
            "jwks": {
                "keys": [
                    {
                        "kty": "EC",
                        "alg": "P-521",
                        "kid": "OJE1cjnUBHGXHtOiHc64gSO1xxNzhoe9sRorb2CCKgU",
                        "x":
 "AV4Ljfyl2eCoP1oyO_U3047BTprKxuwlUm57p7FsQJFMtW1Xks7j8IQe4H0S8tNpd21Q_2NcKiJg5gj
                         WKs0H3Oh6",
                        "y": "AIWYPJ-
c1UWEWQXO4Zkl3TKCPxCiAqv7ju_vJsO0Jye7zC1SzqAFbfIzCRRq_MJJJfmw2ZbfgtvHmG2
                         8avR1O287",
                        "alg": "ES512"
                    }
                ]
            }
        }
    }
}'
```

Pour plus d'informations sur la spécification JSON, reportez-vous à la section https://developer.okta.com/docs/reference/api-overview/

5. Affichez votre application dans la console Okta et copiez l'**ID client**.
6. Attribuez les applications aux utilisateurs. Pour obtenir des instructions, reportez-vous à https://help.okta.com/en/prod/Content/Topics/Provisioning/lcm/lcm-user-app-assign.htm.
7. Pour configurer les revendications d'ID Okta, accédez à **Sécurité** > **API** > **Serveur d'autorisation** et sélectionnez votre serveur d'autorisation.

8. Dans l'onglet **Revendications**, cliquez sur **Ajouter des revendications** et ajoutez une revendication avec les valeurs suivantes :
   a) **Nom** : object_GUID
   b) **Inclure dans le type de jeton** : Jeton ID, Toujours
   c) **Type de valeur** : Expression
   d) **Valeur** : findDirectoryUser().externalId
9. Cliquez sur **Créer**.

Configurer Okta comme un fournisseur d'identité dans BlackBerry UEM

Après avoir créé un client Okta, vous devez créer un fournisseur d'identité correspondant dans la console de gestion BlackBerry UEM.

Avant de commencer : Créer une application Okta

1. Dans la console de gestion BlackBerry UEM, cliquez sur **Paramètres > BlackBerry Enterprise Identity > Fournisseurs d'identité**.
2. Cliquez sur **+** et sélectionnez **Okta**.
3. Dans le champ **Nom**, saisissez un nom pour le fournisseur d'identité.
4. Dans le champ **URL du document découverte OIDC**, entrez l'emplacement du serveur Okta de votre organisation. Par exemple, `https://<oktaDomina>.okta.com/.well-known/oauth-authorization`
5. Dans le champ **ID client**, saisissez le même ID que celui que vous avez créé lors de la tâche Créer une application Okta.
6. Dans le champ **Clé privée JWKS**, saisissez la clé privée que vous avez utilisée lors de la tâche Créer une application Okta.

   Votre saisie doit être similaire à celle-ci :

```
curl --request POST 'https://<oktaDomain>.okta.com/api/v1/apps/' \
--header 'Authorization: SSWS <token>' \
--header 'Content-Type: application/json' \
--data-raw '{
    "name": "oidc_client",
    "label": "BlackBerry Enterprise ID Client",
    "signOnMode": "OPENID_CONNECT",
    "credentials": {
        "oauthClient": {
            "token_endpoint_auth_method": "private_key_jwt"
        }
    },
    "settings": {
        "oauthClient": {
            "redirect_uris": [
                "https://idp.blackberry.com/idp/externalIdpCb"
            ],
            "response_types": [
                "code"
            ],
            "grant_types": [
                "authorization_code"
            ],
            "application_type": "native",
            "jwks": {
                "keys": [
                    {
                        "kty": "EC",
                        "alg": "P-521",
```

```
                        "kid": "OJE1cjnUBHGXHtOiHc64gSO1xxNzhoe9sRorb2CCKgU",
                        "x":
 "AV4Ljfyl2eCoP1oyO_U3047BTprKxuwlUm57p7FsQJFMtW1Xks7j8IQe4H0S8tNpd21Q_2NcKiJg5gj
                         WKs0H3Oh6",
                        "y": "AIWYPJ-
c1UWEWQXO4Zkl3TKCPxCiAqv7ju_vJsO0Jye7zC1SzqAFbfIzCRRq_MJJJfmw2ZbfgtvHmG2
                         8avR1O287",
                        "alg": "ES512"
                    }
                ]
            }
        }
    }
}'
```

7. Dans la liste **Services disponibles**, sélectionnez les services que vous souhaitez attribuer au client Okta et cliquez sur la flèche droite pour déplacer le service dans la liste **Service sélectionné**. Notez que vous ne pouvez attribuer qu'un seul client Okta pour chaque service.
8. Cliquez sur **Enregistrer**.

À la fin : Créer une stratégie d'authentification Enterprise Identity et attribuez-le à des utilisateurs ou à des groupes. Dans la stratégie, ajoutez votre service dans Gérer les exceptions de service et définissez le niveau d'authentification minimal sur le niveau 4.

Gestion des groupes d'applications

Vous pouvez utiliser des groupes d'applications pour créer un ensemble d'applications dans BlackBerry UEM et les attribuer à des utilisateurs, groupes d'utilisateurs ou groupes de terminaux. Les groupes d'applications permettent une gestion plus efficace et plus cohérente des applications. Par exemple, vous pouvez utiliser les groupes d'applications pour grouper la même application pour plusieurs types de terminaux ou pour grouper des applications pour des utilisateurs dotés du même rôle au sein de votre organisation. Avec BlackBerry Enterprise Identity, un groupe d'applications peut également contenir l'autorisation par identification unique en plus des fichiers source d'applications mobiles pour un service spécifique. Ceci vous permet de donner aux utilisateurs tout ce dont ils ont besoin pour accéder à ce service d'un seul coup.

Utilisez la console de gestion BlackBerry UEM pour gérer les différents groupes d'applications. Pour plus d'informations, reportez-vous à la section Gestion des groupes d'applications dans le contenu relatif à l'administration de BlackBerry UEM.

Attribution de droits à des utilisateurs ou groupes

Avant de commencer : Vous devez ajouter des utilisateurs et des services dans BlackBerry UEM avant de pouvoir attribuer à vos utilisateurs des droits d'accès à certains services. Pour plus d'informations sur l'ajout de services, consultez le guide Intégration de services SaaS. Une fois les services Enterprise Identity synchronisés avec BlackBerry UEM, les services sont disponibles dans la console de gestion en tant qu'applications. Vous devez attribuer une application à un utilisateur pour lui donner accès à ce service.

1. Dans la console de gestion BlackBerry UEM, sélectionnez l'utilisateur ou le groupe d'utilisateurs à qui vous souhaitez attribuer des droits. Effectuez l'une des opérations suivantes :
   - Pour attribuer des droits à un utilisateur, dans la barre de menus, cliquez sur **Utilisateurs** et sélectionnez son nom.
   - Pour attribuer des droits à un groupe, dans la barre de menus, cliquez sur **Groupes** et sélectionnez le groupe. Cliquez sur l'onglet **Paramètres**.
2. Sélectionnez l'application ou le groupe d'applications à attribuer.
3. Cliquez sur la case en regard du service que vous souhaitez attribuer.
4. Cliquez sur **Attribuer**.
5. Si vous êtes invité à attribuer des licences, cliquez sur **Oui**.

Modifier les paramètres Enterprise Identity

Certains paramètres BlackBerry Enterprise Identity sont réglables à partir de la console de gestion BlackBerry UEM. Vous pouvez modifier le nom d'affichage des informations d'identification sur la page de connexion Enterprise Identity. Vous pouvez également modifier le classement des authentificateurs. Le processus d'authentification des services démarre avec l'authentificateur le mieux classé et ainsi de suite.

1. Dans la barre de menus, cliquez sur **Paramètres** > **BlackBerry Enterprise Identity**.
2. Vous pouvez saisir ou modifier le nom d'utilisateur convivial de vos informations d'identification BlackBerry UEM dans la zone de texte Nom.
3. Pour modifier le classement des authentificateurs, cliquez sur les flèches montante et descendante de la colonne **Classement**. Mobile ZSO n'est pas pris en charge par tous les services. Ainsi, si cet authentificateur est placé en haut de la colonne, certains services ne seront pas disponibles.
4. Cliquez sur **Enregistrer**.

Personnaliser la page de connexion de l'utilisateur de votre entreprise

Vous pouvez personnaliser votre page de connexion de l'utilisateur de votre entreprise BlackBerry Enterprise Identity. Par exemple, vous pouvez ajouter le logo de votre entreprise.

1. Sur la console de gestion BlackBerry UEM, dans la barre de menus, cliquez sur **Applications**.
2. Cliquez sur **Ajouter une application**.
3. Cliquez sur **Enterprise Identity**. Un message vous demandant de synchroniser les services Enterprise Identity s'affiche.
4. Cliquez sur **Ouvrir la console Enterprise Identity**. La console d'administration s'ouvre dans un nouvel onglet de navigateur. Si la console ne s'ouvre pas, vérifiez que vous avez activé les fenêtres contextuelles dans votre navigateur.
5. Cliquez sur **Enterprise**.
6. Dans le champ **Texte de sécurité de connexion**, entrez toutes les informations supplémentaires que vous fournir à vos utilisateurs. Ce texte s'affichera sous le champ Mot de passe sur la page de connexion.
7. Dans le champ **Titre de connexion**, tapez le texte qui s'affichera en haut de la page de connexion BlackBerry Enterprise Identity de votre organisation. Vous pouvez utiliser la liste déroulante **Insérer jeton** pour formater le texte du titre de connexion.
8. Dans le champ **Description du nom d'utilisateur**, tapez le texte qui s'affichera au-dessus du champ de texte Nom d'utilisateur sur la page de connexion BlackBerry Enterprise Identity de votre organisation. Vous pouvez utiliser la liste déroulante **Insérer jeton** pour formater le texte de la description du nom d'utilisateur.
9. Dans le champ **Description du mot de passe**, tapez le texte qui s'affichera au-dessus du champ de texte Mot de passe sur la page de connexion BlackBerry Enterprise Identity de votre organisation. Vous pouvez utiliser la liste déroulante **Insérer jeton** pour formater le texte de description du mot de passe.
10. Dans le champ **Logo**, cliquez sur **Choisir le fichier** pour rechercher et ajouter un logo à la page de connexion BlackBerry Enterprise Identity de votre organisation.
11. Choisissez des options pour les champs **Style du logo**, **Option de couleur du texte**, et **Arrière-plan**.
12. Cliquez sur **Enregistrer**.

Prise en charge de SAML ECP pour Microsoft Office 365

Certains clients de messagerie, y compris certaines versions de BlackBerry Hub et BlackBerry Work, ne prennent pas en charge l'interface Microsoft ADAL lorsqu'elle est utilisée avec Microsoft Office 365, ce qui empêche BlackBerry Enterprise Identity d'afficher son interface utilisateur de connexion normale. Pour activer ces clients de messagerie mobile, vous pouvez activer la prise en charge ECP (Enhanced Client or Proxy Profile) de Enterprise Identity pour Office 365, ce qui permet l'authentification avec des informations d'identification textuelles, telles que le nom d'utilisateur et le mot de passe. Ces informations sont généralement recueillies à partir de l'interface utilisateur du client de messagerie. Notez que lorsque ECP est utilisé pour Office 365, les politiques d'authentification Enterprise Identity ne s'appliquent pas aux connexions basées sur ECP.

Activation de la prise en charge ECP pour Office 365

1. Dans la barre de menu de la console de gestion BlackBerry UEM, cliquez sur **Applications**.
2. Cliquez sur **Ajouter une application**.
3. Cliquez sur **Enterprise Identity**.
4. Cliquez sur **Ouvrir la console Enterprise Identity**. La console d'administration s'ouvre dans un nouvel onglet de navigateur. Si la console ne s'ouvre pas, vérifiez que vous avez activé les fenêtres contextuelles dans votre navigateur.
5. Sur la page **Entreprise**, définissez l'option **Prise en charge ECP pour Microsoft Office 365** sur **Activée**.
6. Cliquez sur **Enregistrer**.

Empêcher les utilisateurs d'être bloqués de leur compte

Vous pouvez configurer BlackBerry Enterprise Identity de façon à empêcher des utilisateurs, tels que les utilisateurs d'Active Directory, d'être bloqués de leur compte en raison d'un trop grand nombre d'échecs de tentatives de connexions à BlackBerry Enterprise Identity.

1. Dans la barre de menu de la console de gestion BlackBerry UEM, cliquez sur **Applications**.
2. Cliquez sur **Ajouter une application**.
3. Cliquez sur **Enterprise Identity**. Un message vous demandant de synchroniser les services Enterprise Identity s'affiche.
4. Cliquez sur **Ouvrir la console Enterprise Identity**. La console d'administration s'ouvre dans un nouvel onglet de navigateur. Si la console ne s'ouvre pas, vérifiez que vous avez activé les fenêtres contextuelles dans votre navigateur.
5. Cliquez sur **Enterprise**.
6. Dans la section **Paramètres de verrouillage de compte**, activez l'option **Activer le verrouillage de compte**.
7. Définissez les options suivantes :
   - **Seuil de tentative de connexion** : définit le nombre d'échecs de tentatives avant le verrouillage temporaire du compte.
   - **Durée de connexion (en minutes**) : définit la durée de verrouillage du compte en minutes. Lorsque ce délai est dépassé, le compte doit être débloqué pour la prochaine tentative de connexion.
   - **Réinitialiser la durée (en minutes)** : définit le nombre de minutes devant s'écouler après l'échec d'une tentative de connexion avant que le compteur soit réinitialisé à 0.
8. Cliquez sur **Enregistrer**.

Sélection de locataire et de domaine

La plupart des utilisateurs se connectent à Enterprise Identity avec un nom d'utilisateur et un mot de passe et spécifient s'il faut faire confiance ou non au navigateur. Si un nom d'utilisateur existe dans plusieurs locataires ou domaines, l'utilisateur devra, lors de sa première connexion, sélectionner le locataire dans une liste déroulante ou saisir le domaine. Les sélections sont enregistrées pour les connexions ultérieures.

Gestion des locataires BlackBerry UEM dans la console BlackBerry Enterprise Identity

Vous pouvez utiliser la page Locataires UEM dans la console Enterprise Identity pour gérer les locataires BlackBerry UEM de votre organisation. Vous pouvez modifier les propriétés des locataires ou désactiver les locataires. Notez que si vous désactivez un locataire, les utilisateurs de votre organisation ne seront en mesure de s'authentifier auprès d'aucun service Enterprise Identity que vous avez activé dans BlackBerry UEM.

Vous pouvez modifier les propriétés suivantes des locataires BlackBerry UEM.

Élément	Description
Nom d'affichage	Modification du nom d'affichage du locataire. Ce nom s'affiche dans le sélecteur de locataires UEM sur l'écran de connexion lorsqu'un utilisateur existe dans plusieurs locataires UEM.
Type d'authentificateur - AD	Activation/désactivation de l'instance Microsoft Active Directory associée et changement du nom d'affichage de l'instance Active Directory.
Types d'authentificateur - LDAP	Activation/désactivation de l'annuaire LDAP associé et changement de son nom d'affichage.
Détection du réseau de travail	Activation/désactivation de la détection du réseau. Ce facteur de risque détermine si l'application ou le navigateur d'un utilisateur est connecté(e) au même réseau que le serveur BlackBerry UEM.

Gérer des administrateurs et des utilisateurs

Vous pouvez ajouter ou supprimer des administrateurs et des utilisateurs, ou modifier leurs droits dans la console de gestion BlackBerry UEM. Pour plus d'informations sur la gestion des administrateurs et des utilisateurs, reportez-vous au contenu relatif à l'administration de BlackBerry UEM.

Si vous devez redéployer BlackBerry UEM pour quelque raison que ce soit, vous devez d'abord supprimer tous les utilisateurs disposant d'autorisations Enterprise Identity à partir de BlackBerry UEM. Si des utilisateurs ne sont pas supprimés avant le redéploiement de BlackBerry UEM, des services peuvent toujours leur être attribués, mais ils ne pourront pas y accéder.

Créer un administrateur Enterprise Identity personnalisé

Vous pouvez utiliser des rôles d'administrateur pour déléguer des tâches administratives BlackBerry Enterprise Identity spécifiques aux utilisateurs. Dans BlackBerry UEM, le rôle Administrateur de sécurité dispose des autorisations maximales sur la console de gestion, y compris sur la création et la gestion de rôles et d'administrateurs. Au moins un administrateur doit être Administrateur de sécurité. BlackBerry UEM inclut des rôles préconfigurés, en plus du rôle Administrateur de sécurité. Vous pouvez modifier ou supprimer tous les rôles, à l'exception du rôle Administrateur de sécurité. Vous pouvez également créer des rôles personnalisés.

Remarque : Les nouveaux administrateurs personnalisés BlackBerry Enterprise Identity que vous créez n'ont pas la possibilité d'attribuer des droits BlackBerry Enterprise Identity ou d'attribuer des applications et groupes d'applications aux utilisateurs ou groupes d'utilisateurs. Pour plus d'informations, reportez-vous aux rubriques Attribuer des droits aux utilisateurs ou groupes et Gestion des groupes d'applications.

Avant de commencer :

- Vous devez être Administrateur de sécurité pour créer un rôle personnalisé.

1. Dans le menu de gauche, cliquez sur **Paramètres > Administrateurs > Rôles**.
2. Cliquez sur  .
3. Saisissez le nom et la description du rôle.
4. Dans la section **Stratégies et profils**, sélectionnez les options de stratégie Enterprise Identity. Vous avez le choix entre : **Afficher la stratégie d'authentification Enterprise Identity, Créer/Modifier la stratégie d'authentification, Supprimer la stratégie d'authentification** et **Attribuer la stratégie d'authentification à des utilisateurs et des groupes**.
5. Dans la section **Paramètres**, sélectionnez les options Enterprise Identity. Vous avez le choix entre : **Afficher les paramètres d'entreprise Enterprise Identity, Modifier les paramètres d'entreprise Enterprise Identity, Afficher les services Enterprise Identity** et **Modifier les services Enterprise Identity**.
6. Cliquez sur **Enregistrer**.
7. Ajoutez le rôle à un compte d'utilisateur ou à un groupe d'utilisateurs.

À la fin :

Pour plus d'informations sur les rôles, consultez le BlackBerry UEM ontenu relatif à l'administration.

Informations juridiques

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 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
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada