BlackBerry AtHoc

Identification unique

7.17

Contents

Activer l'authentification unique en tant que méthode d'authentification

La fonctionnalité d'authentification unique n'est pas activée par défaut. Un administrateur système doit activer l'authentification unique dans les paramètres d'activation des fonctionnalités du système de gestion BlackBerry® AtHoc®. Pour plus d'informations, reportez-vous à la section Activer et désactiver les fonctionnalités du guide *BlackBerry AtHoc Paramètres et configuration du système*.

Lorsque la SSO est activée pour votre entreprise, si vos utilisateurs sont déjà authentifiés et connectés à l'aide de votre fournisseur d'identité (IDP), ils n'ont pas besoin de se reconnecter pour accéder au système de gestion BlackBerry AtHoc ou à Self-Service.

Note: L'authentification unique est prise en charge sur l'application de bureau lorsque la méthode d'authentification est définie sur « Reporter à Self-Service » et que Self-Service est activé pour l'authentification unique.

Si un utilisateur n'est pas connecté, il est redirigé vers le nom de connexion IDP du client de son entreprise lorsqu'il tente de se connecter. Cet IDP est géré par votre organisation ou par un fournisseur tiers qui fournit des services IDP. L'IDP authentifie l'utilisateur. L'utilisateur est ensuite redirigé vers BlackBerry AtHoc. Si l'utilisateur est déjà connecté à l'IDP, il est automatiquement redirigé vers le système de gestion BlackBerry AtHoc ou Self-Service avec une session active.

Vous devez être un administrateur d'organisation, un administrateur d'entreprise ou un administrateur système pour activer l'authentification unique en tant que méthode d'authentification de l'utilisateur.

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur.
2. Dans la barre de navigation, cliquez sur .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Dans la fenêtre **Authentification de l'utilisateur**, dans la section **Méthodes d'authentification activées**, cochez la case **Activer l'authentification unique (SSO)**.
5. Cliquez sur **Enregistrer**.

Activer l'authentification unique pour Self-Service

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur.
2. Dans la barre de navigation, cliquez sur .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Dans la fenêtre **Authentification de l'utilisateur**, dans la section **Attribuer des méthodes d'authentification aux applications**, dans la section **Self-Service**, sélectionnez **Authentification unique** dans la liste **Méthode d'authentification**. Le champ URL de connexion est automatiquement renseigné avec une URL au format suivant : <*server*>/selfservice/*organization-code*. Cette URL est utilisée lorsque les utilisateurs tentent d'accéder à Self-Service à l'aide de l'authentification SSO.
5. Si vous avez sélectionné **Authentification unique** comme méthode d'authentification, vous pouvez également sélectionner **Nom d'utilisateur et Mot de passe** dans la liste **Autres méthodes d'authentification** pour activer à la fois l'authentification SSO et l'authentification des utilisateurs par nom d'utilisateur/mot de passe.

   Note: Lorsqu'une autre méthode d'authentification est ajoutée, l'URL d'ouverture de session de Self-Service est ajoutée avec /sso pour l'authentification unique. Par exemple, <*server*>/selfservice/*organization-code*/sso.
6. Cliquez sur **Configuration**.

   Note: Si le bouton **Configuration** n'est pas disponible, l'authentification unique n'est pas activée. Pour plus d'informations, reportez-vous à Activer l'authentification unique en tant que méthode d'authentification.

7. Dans la fenêtre **Configuration de la SSO de Self-Service**, exportez les paramètres SP et IDP, puis importez les paramètres IDP.

   Note: Vous pouvez également configurer manuellement les paramètres IDP et SP. Pour plus d'informations, reportez-vous aux sections Configurer les paramètres de fournisseur d'identité et Configurer les paramètres du fournisseur de services.
8. Cliquez sur **Apply** (Appliquer).
9. Cliquez sur **Enregistrer**.

Activer l'authentification unique pour le système de gestion BlackBerry AtHoc

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur.
2. Dans la barre de navigation, cliquez sur .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Dans la fenêtre **Authentification de l'utilisateur**, dans la section **Attribuer des méthodes d'authentification aux applications**, dans la section **Gestion du système**, sélectionnez **Authentification unique** dans la liste **Méthode d'authentification**. Le champ URL de connexion est automatiquement renseigné avec une URL au format suivant : <*server*>/client/*organization-code*. Cette URL est utilisée lorsqu'un utilisateur tente d'accéder au système de gestion BlackBerry AtHoc à l'aide de l'authentification SSO.

   Note: Si la liste **Méthode d'authentification** est désactivée, la SSO n'est pas activée. Pour plus d'informations, reportez-vous à Activer l'authentification unique en tant que méthode d'authentification.
5. Cliquez sur **Configuration**.
6. Dans la fenêtre **Configuration de la SSO de gestion du système**, exportez les paramètres SP et IDP, puis importez les paramètres IDP.

   Note: Vous pouvez également configurer manuellement les paramètres IDP et SP. Pour plus d'informations, reportez-vous aux sections Configurer les paramètres de fournisseur d'identité et Configurer les paramètres du fournisseur de services.
7. Cliquez sur **Apply** (Appliquer).
8. Cliquez sur **Enregistrer**.

Importer un certificat de fournisseur de services

Importez un certificat de fournisseur de services signé BlackBerry AtHoc pour l'utiliser dans l'authentification unique (SSO). Cela permet aux administrateurs de sélectionner un certificat BlackBerry AtHoc au lieu de télécharger et de gérer un certificat SP personnalisé.

Vous devez être un administrateur système pour importer un certificat de fournisseur de services.

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur système.
2. Passez à l'organisation **Configuration du système (3)**.
3. Dans la barre de navigation, cliquez sur .
4. Dans la section **Configuration du système**, cliquez sur **Politique de sécurité**.
5. Sur la page **Stratégie de sécurité**, dans la section **Certificat du fournisseur de services**, cliquez sur **Importer le certificat**.
6. Dans la fenêtre **Importer le certificat**, saisissez un mot de passe valide pour le certificat du fournisseur de services.
7. Cliquez sur **Parcourir** et accédez à un certificat BlackBerry AtHoc valide et sélectionnez-le. Seuls les fichiers .pfx et .p12 peuvent être importés.
8. Cliquez sur **Importer**.
9. Sur la page **Stratégie de sécurité**, cliquez sur **Enregistrer**.

Configurer les paramètres de fournisseur d'identité

Le fournisseur d'identité (IDP) assure l'authentification des utilisateurs. Dans ce cas, le fournisseur de services (SP), BlackBerry AtHoc ou Self-Service, demande l'authentification au fournisseur d'identité.

Lorsque l'authentification SSO est activée pour l'accès au système de gestion BlackBerry AtHoc ou à Self-Service, lorsqu'un utilisateur se connecte, il est redirigé vers l'IDP de son organisation pour authentification. Si l'utilisateur est déjà connecté au fournisseur d'identité, la demande d'authentification est traitée et envoyée au fournisseur de services, et l'accès est accordé à l'utilisateur sans qu'il soit nécessaire de se reconnecter.

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur de l'organisation ou administrateur d'entreprise.
2. Cliquez sur  .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Sur la page **Authentification de l'utilisateur**, dans la section **Attribuer des méthodes d'authentification aux applications** de la section **Self-Service** ou **Système de gestion**, cliquez sur **Configuration**.

   Note: Si le bouton **Configuration** n'est pas disponible, l'authentification unique n'est pas activée. Pour plus d'informations, reportez-vous à Activer l'authentification unique en tant que méthode d'authentification.
5. Effectuez l'une des opérations suivantes :

   - Importer les paramètres IDP.
   - Dans la fenêtre **Configuration SSO du système de gestion** ou **Configuration SSO de Self-Service**, dans la section **Fournisseur d'identité**, configurez les **Paramètres généraux** suivants.

     a. **Nom du fournisseur d'identité** : Chaque configuration SAML est identifiée par un nom de fournisseur d'identité unique. Ce nom est interne à la configuration et n'est pas exposé aux fournisseurs partenaires. Ce champ est obligatoire uniquement lorsqu'il existe plusieurs configurations SAML. Saisissez un nom composé de trois caractères minimum et de 512 caractères maximum. Les caractères spéciaux suivants ne sont pas autorisés : `!?"<>!$%&^()={},;\:?"<>
     b. **URL du service d'ouverture de session** : Saisissez l'URL de l'emplacement du service SSO du fournisseur d'identité où les demandes d'authentification SAML sont envoyées dans le cadre d'une authentification unique initiée par le fournisseur de services.
     c. **Liaison au service d'ouverture de session** : En option, sélectionnez **Rediriger** ou **POST** comme mécanisme de transport (liaison SAML) à utiliser lors de l'envoi de demandes d'authentification SAML au fournisseur d'identité partenaire. Le paramètre par défaut est **Rediriger**.
     d. **URL du service de déconnexion** : URL du service de déconnexion unique du fournisseur de services local où les messages de déconnexion SAML sont reçus. Si une déconnexion unique n'est pas nécessaire, laissez ce champ vide. Pour plus d'informations, reportez-vous à Service de déconnexion SSO.
     e. **Liaison au service de déconnexion** : En option, sélectionnez **Rediriger** ou **POST** comme mécanisme de transport (liaison SAML) à utiliser lors de l'envoi de demandes d'authentification SAML au fournisseur d'identité partenaire. Le paramètre par défaut est **Rediriger**.
     f. **URL du service de résolution d'artéfacts** : Vous pouvez également saisir une URL de service de résolution d'artéfacts. Le fournisseur de services utilise le protocole de résolution d'artéfacts pour échanger un artéfact contre le message SAML réel référencé par l'artéfact.
     g. **Liaison au service de résolution d'artéfacts** : Vous pouvez également sélectionner **SOAP**, **POST**, **REDIRIGER** ou **ARTÉFACT** comme mécanisme de transport (liaison SAML) à utiliser lors de l'envoi de demandes d'authentification SAML au fournisseur d'identité partenaire. La valeur par défaut est **SOAP**.
     h. **Format de l'ID du nom** : Si vous le souhaitez, sélectionnez **Adresse e-mail**, **Persistant** ou **Transitoire** comme format à utiliser par le SP et l'IDP pour identifier un identifiant de nom d'objet.
     i. **Attribut de mappage utilisateur** : Vous pouvez également sélectionner l'attribut qui identifie l'utilisateur. Cet attribut est récupéré à partir des métadonnées d'assertion SAML. La valeur par défaut est **Nom du sujet**.

j. **Nom de l'attribut** : Saisissez le nom de l'attribut utilisé pour identifier l'utilisateur.

6. Configurez les **Paramètres de sécurité** suivants :
   a. **Signature de réponse SAML** : Sélectionnez **Signé** ou **Non signé**. Lorsque vous sélectionnez **Signé**, les réponses SAML envoyées au fournisseur de services partenaire doivent être signées. L'envoi de demandes d'authentification signées est fortement recommandé, mais facultatif.
   b. **Signature d'assertion** : Sélectionnez **Signé** ou **Non signé**. Lorsque vous sélectionnez **Signé**, les assertions SAML envoyées au fournisseur de services partenaire doivent être signées.

      Note:

      - Vous devez sélectionner **Signé** dans **Signature de réponse SAML**, **Signature d'assertion** ou les deux.
      - Un certificat valide doit être installé pour votre organisation.

   c. **Algorithme de signature** : Sélectionnez un algorithme. La valeur par défaut est **RSA-SHA256**.
   d. **Chiffrement d'assertion** : Sélectionnez **Chiffré** ou **Non chiffré**. Lorsque vous sélectionnez **Chiffré**, les assertions SAML envoyées au fournisseur de services partenaire doivent être chiffrées.
   e. Si **Chiffrement d'assertion** est défini sur **Chiffré**, sélectionnez un **Algorithme d'assertion**. Le paramètre par défaut est **AES128**.
   f. Dans le champ **Certificat***, cliquez sur **Parcourir** pour rechercher et sélectionner un fichier de certificat. Seuls les fichiers .cer et .crt sont pris en charge.
7. Vous pouvez également ajouter les **informations supplémentaires** suivantes :
   a. **Nom de l'entreprise** : Saisissez un nom composé de trois caractères minimum et de 512 caractères maximum. Les caractères spéciaux suivants ne sont pas autorisés : `!?"<>!$%&^()={},;\:?"<>
   b. **Nom d'affichage de l'entreprise** : Saisissez un nom composé de trois caractères minimum et de 512 caractères maximum. Les caractères spéciaux suivants ne sont pas autorisés : `!?"<>!$%&^()={},;\:?"<>
   c. **URL de l'entreprise**
   d. **Nom de la personne à contacter**
   e. **Rôle ou service**
   f. **Adresse e-mail**
   g. **Numéro de téléphone**
8. Effectuez l'une des opérations suivantes :
   - Si vous modifiez une configuration SSO existante, cliquez sur **Appliquer**, puis sur **Enregistrer** sur la page **Authentification de l'utilisateur**.
   - Pour une nouvelle configuration SSO, configurez les paramètres du fournisseur de services.

Configurer les paramètres du fournisseur de services

1. Connectez-vous au système de gestion BlackBerry AtHoc en tant qu'administrateur de l'organisation ou administrateur d'entreprise.
2. Cliquez sur .
3. Dans la section **Utilisateurs**, cliquez sur **Authentification de l'utilisateur**.
4. Sur la page **Authentification de l'utilisateur**, dans la section **Attribuer des méthodes d'authentification aux applications** de la section **Self-Service** ou **Système de gestion**, cliquez sur **Configuration**.
5. Dans la fenêtre **Configuration SSO du système de gestion** ou **Configuration SSO de Self-Service**, faites défiler jusqu'à la section **Fournisseur de services**.
6. Configurez les **Paramètres généraux** suivants :
   a. **Nom du fournisseur de services** : Saisissez le nom du fournisseur de services qui envoie la demande d'authentification SAML. Saisissez un nom composé de trois caractères minimum et de 512 caractères maximum. Les caractères spéciaux suivants ne sont pas autorisés : `!?"<>!$%&^()={},,\:?"<>
   b. **URL du service de respect du consommateur** : Ce champ est prérempli avec l'URL du point de terminaison du fournisseur de services qui reçoit le SAML du fournisseur d'identité. L'URL du service de respect du consommateur est ajoutée au code de l'organisation. Par exemple :
      - URL Self-Service : `https://domain/SelfService/Account/NewSSO/organization-code`
      - Système de gestion BlackBerry AtHoc : `https://domain/Client/organization-code`
   c. **URL du service de déconnexion** : Ce champ est prérempli avec l'URL du point de terminaison du fournisseur de services qui reçoit les messages de déconnexion SAML. Pour plus d'informations, reportez-vous à Service de déconnexion SSO.
   d. **URL de déconnexion personnalisée** : Vous pouvez également saisir une URL personnalisée vers laquelle rediriger les utilisateurs lors de la déconnexion.
   e. **Liaison au service de déconnexion personnalisé** : En option, sélectionnez **POST** ou **Rediriger** comme mécanisme de transport (liaison SAML) à utiliser lors de l'envoi de demandes d'authentification SAML à l'IDP partenaire. Le paramètre par défaut est **POST**.
7. Configurez les **Paramètres de sécurité** suivants :
   a. **Signature de requête SAML** : Sélectionnez **Signé** ou **Non signé**. Lorsque l'option **Signé** est sélectionnée, les requêtes d'authentification SAML reçues du fournisseur de services partenaire doivent être signées. La réception des requêtes d'authentification signées est facultative, mais fortement recommandée.
   b. Si **Signature de requête SAML** est définie sur **Signé**, sélectionnez **Algorithme de signature**. Le paramètre par défaut est **RSA-SHA256**.
   c. Dans la section **Certificat***, procédez d'une des manières suivantes :
      - Sélectionnez **Utiliser le certificat BlackBerry** pour utiliser le certificat BlackBerry signé.

        Note: Un administrateur système doit télécharger un certificat signé BlackBerry valide pour que cette option s'affiche.
      - Sélectionnez **Utiliser le certificat personnalisé** et cliquez sur **Importer le certificat**. Dans la fenêtre **Importer le certificat**, saisissez un mot de passe et cliquez sur **Parcourir**. Accédez au fichier du certificat valide et sélectionnez-le. Cliquez sur **Importer**. Seuls les types de fichiers .pfx et .p12 sont pris en charge.
8. Cliquez sur **Apply** (Appliquer).
9. Sur la page **Authentification de l'utilisateur**, cliquez sur **Enregistrer**.

Service de déconnexion SSO

Si l'URL de déconnexion est configurée dans les paramètres du fournisseur d'identité, les étapes suivantes mettent fin à la session utilisateur active :

1. L'utilisateur lance une demande de déconnexion auprès d'un fournisseur de services.
2. Le fournisseur de services transfère la demande de déconnexion à un fournisseur d'identité.
3. Le fournisseur d'identité valide la demande de déconnexion.
4. Le fournisseur d'identité envoie une demande de déconnexion de l'utilisateur à tous les autres fournisseurs de services avec lesquels le fournisseur d'identité est conscient que l'utilisateur dispose d'une session de sécurité active.
5. Le fournisseur d'identité met fin aux sessions de l'utilisateur et envoie une réponse au fournisseur de services d'origine.
6. Le fournisseur de services d'origine informe l'utilisateur qu'il a été déconnecté.

Si l'URL de déconnexion s'affiche dans les paramètres du fournisseur de services, les étapes suivantes mettent fin à la session utilisateur active :

1. L'utilisateur lance une demande de déconnexion auprès d'un fournisseur de services.
2. Le fournisseur de services met fin à toutes les sessions actives de l'utilisateur qui sont gérées par un service tiers.
3. Le fournisseur de services transfère la demande de déconnexion à l'URL de déconnexion.

Si l'URL de déconnexion n'est pas configurée pour le fournisseur d'identité ou le fournisseur de services, lorsqu'un utilisateur demande une déconnexion, le fournisseur de services met fin à la session active de l'utilisateur et affiche la page de connexion (pour le système de gestion BlackBerry AtHoc) ou la page de déconnexion (pour Self Service).

Le tableau suivant décrit les flux de déconnexion du système de gestion BlackBerry AtHoc :

Type de déconnexion	Initiateur	URL de déconnexion IDP incluse	URL de déconnexion personnalisée disponible	Comportement de déconnexion
Déconnexion ou expiration de session	SP	Oui	Oui	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers l'URL de connexion SSO de son organisation. L'URL de déconnexion IDP est utilisée.

Type de déconnexion	Initiateur	URL de déconnexion IDP incluse	URL de déconnexion personnalisée disponible	Comportement de déconnexion
Déconnexion ou expiration de session	SP	Oui	Non	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers l'URL de connexion SSO de son organisation. L'URL de déconnexion IDP est utilisée.
Déconnexion ou expiration de session	SP	Non	Oui	L'utilisateur final est déconnecté localement et redirigé vers l'URL de déconnexion personnalisée.
Déconnexion ou expiration de session	SP	Non	Non	L'utilisateur final est déconnecté localement et redirigé vers l'URL de connexion SSO de l'organisation.
Délai d'expiration de la session	IDP	Oui	Oui	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de connexion manuelle avec un message d'expiration de session.

Type de déconnexion	Initiateur	URL de déconnexion IDP incluse	URL de déconnexion personnalisée disponible	Comportement de déconnexion
Délai d'expiration de la session	IDP	Oui	Non	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de connexion manuelle avec un message d'expiration de session.
Déconnexion ou expiration de session	IDP	Non	Oui	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers l'URL de déconnexion personnalisée.
Délai d'expiration de la session	IDP	Non	Non	L'utilisateur final est déconnecté localement et redirigé vers la page de connexion manuelle avec un message d'expiration de session.
Déconnexion	IDP	Oui	Oui	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de connexion manuelle.

Type de déconnexion	Initiateur	URL de déconnexion IDP incluse	URL de déconnexion personnalisée disponible	Comportement de déconnexion
Déconnexion	IDP	Oui	Non	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de connexion manuelle.
Déconnexion	IDP	Non	Non	L'utilisateur final est déconnecté localement et redirigé vers la page de connexion manuelle.

Le tableau suivant décrit les flux de déconnexion pour Self-Service :

Type de déconnexion	Initiateur	URL de déconnexion IDP incluse	URL de déconnexion personnalisée incluse	Comportement de déconnexion
Déconnexion ou expiration de session	SP	Oui	Oui	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de déconnexion.
Déconnexion ou expiration de session	SP	Oui	Non	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de déconnexion.
Déconnexion ou expiration de session	SP	Non	Oui	L'utilisateur final est déconnecté localement et redirigé vers l'URL personnalisée.

Type de déconnexion	Initiateur	URL de déconnexion IDP incluse	URL de déconnexion personnalisée incluse	Comportement de déconnexion
Déconnexion ou expiration de session	SP	Non	Non	L'utilisateur final est déconnecté localement et redirigé vers la page de déconnexion.
Déconnexion ou expiration de session	IDP	Oui	Oui	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de déconnexion. Le bouton **Aller à la page de connexion** n'est pas visible.
Déconnexion ou expiration de session	IDP	Oui	Non	La session IDP est terminée. L'utilisateur final est déconnecté localement et redirigé vers la page de déconnexion. Le bouton **Aller à la page de connexion** n'est pas visible.
Déconnexion ou expiration de session	IDP	Non	Oui	L'utilisateur final est déconnecté localement et redirigé vers l'URL personnalisée.
Déconnexion ou expiration de session	IDP	Non	Non	L'utilisateur final est déconnecté localement et redirigé vers la page de déconnexion.

Exporter les paramètres SP et IDP

Lorsque vous configurez l'authentification unique, vous pouvez exporter les données de paramètres à partir du IDP et du SP au lieu de saisir manuellement ces informations.

1. Dans la fenêtre **Configuration SSO du système de gestion** ou **Configuration SSO de Self-Service**, dans la section **Fournisseur d'identité**, dans les **Paramètres généraux**, cliquez sur **Exporter**. Les paramètres IDP sont téléchargés dans un fichier .xml. Naviguez pour sélectionner un emplacement sur votre ordinateur local où enregistrer le fichier.
2. Dans la fenêtre **Configuration SSO du système de gestion** ou **Configuration SSO de Self-Service**, dans la section **Fournisseur de services**, dans les **Paramètres généraux**, cliquez sur **Exporter**.

   Note: Les informations de mot de passe et de clé privée sont exclues des exportations de métadonnées du fournisseur de services.

   Les paramètres SP sont téléchargés dans un fichier .xml. Naviguez pour sélectionner un emplacement sur votre ordinateur local où enregistrer le fichier.
3. Cliquez sur **Enregistrer**.

Importer les paramètres IDP

Lors de la configuration de la SSO, vous pouvez exporter puis importer les données de paramètres depuis le fournisseur d'identité au lieu de saisir manuellement ces informations.

1. Dans la fenêtre **Configuration SSO du système de gestion** ou **Configuration SSO de Self-Service**, dans la section **Fournisseur d'identité**, dans les **Paramètres généraux**, cliquez sur **Importer**.
2. Dans la fenêtre **Importer la configuration du fournisseur d'identité**, cliquez sur **Parcourir** pour sélectionner le fichier .xml contenant votre configuration IDP.
3. Cliquez sur **Ouvrir**.
4. Cliquez sur **Importer**. Les champs de la section Fournisseur d'identité sont renseignés avec les données du fichier .xml importé. Si des champs ont été remplis avant l'importation, ils sont surchargés. Si le fichier .xml contient des champs non valides, une erreur s'affiche et aucun paramètre n'est importé.
5. Cliquez sur **Apply** (Appliquer).

Importer une configuration IDP existante

Si vous disposez déjà d'une implémentation SSO basée sur une base de données et que vous souhaitez migrer vers la solution SSO améliorée basée sur l'interface utilisateur, vous pouvez migrer la configuration des paramètres depuis votre IDP et l'importer dans le système de gestion BlackBerry AtHoc.

Contactez votre représentant de compte ou le support client BlackBerry AtHoc pour obtenir une copie du fichier `Utilities.zip` nécessaire à la migration SSO.

Note: Seules les configurations IDP peuvent être importées. La configuration SP doit être saisie manuellement dans le système de gestion BlackBerry AtHoc. Reportez-vous à la section Configurer les paramètres du fournisseur de services.

1. Ouvrez une invite de commande Windows et accédez au dossier suivant :

   ```
   <installed-directory>\AtHocENS\ServerObjects\Tools\SSO\EasyConnect
   ```

2. Exécutez la commande suivante pour créer et exporter un fichier XML de métadonnées SAML :

   ```
   ExportMetadata.exe –partner <name> [-config <directoryName] [-baseurl <url>] [-file <filename>]
   ```

   où :

   - partner <*name*>: Nom de l'IDP partenaire configuré dans le fichier `idp-partner.config` ou du SP partenaire configuré dans le fichier `sp-partner.config`.
     - Si vous spécifiez un IDP partenaire, les métadonnées du SP local correspondant sont générées pour le IDP partenaire.
     - Si vous spécifiez un SP partenaire, les métadonnées du IDP local correspondant sont générées pour le SP partenaire.
   - [-baseurl <*url*>]: Spécifiez le répertoire contenant les fichiers de configuration EasyConnect. Si vous ne spécifiez pas ce répertoire, l'exportation est définie par défaut sur C:\EasyConnect\EasyConnectServer.
   - [-file <*filename*>]: Vous pouvez également spécifier le nom du fichier de métadonnées SAML généré. Par défaut, l'exportation utilise le nom de fichier metadata.xml.

     Exemples :

     - ExportMetadata.exe –partner ExampleIdentityProvider
     - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory"**
     - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory" -baseurl "HTTPS://www.showcase.com"*
     - ExportMetadata.exe –partner ExampleIdentityProvider config "specify SSO config directory" -baseurl "HTTPS://www.showcase.com" -file "<File path>"**

3. Connectez-vous au système de gestion BlackBerry AtHoc et utilisez la fonctionnalité d'importation SSO IDP pour importer les métadonnées IDP. Voir Exporter les paramètres SP et IDP et Importer les paramètres IDP.

Activer la vérification de la liste de révocation de certificat SSO

Lorsque l'authentification unique est activée pour votre organisation, une CRL est conservée. Une CRL est une liste de certificats numériques qui ont été révoqués et qui ne doivent pas être approuvés. Si la vérification des CRL est activée, BlackBerry AtHoc vérifie la CRL avant de lancer une requête d'authentification SAML auprès d'un fournisseur d'identité ou après avoir reçu une réponse SAML de l'IDP.

1. Dans la barre de navigation, cliquez sur .
2. Dans la section **Configuration du système**, cliquez sur **Politique de sécurité**.
3. Dans la section **Paramètres SSO de la CRL (liste de révocation de certificats)**, sélectionnez l'option **Activer la vérification des CRL**.

   Note: Si la section **Paramètres SSO de la CRL (liste de révocation de certificats)** n'est pas visible, l'authentification unique n'est pas activée. Voir Activer l'authentification unique pour Self-Service et Activer l'authentification unique pour le système de gestion BlackBerry AtHoc.
4. Dans le champ **Délai d'expiration de la CRL**, saisissez le nombre de secondes pendant lesquelles les informations de validation du certificat peuvent être récupérées à partir de l'autorité de certification. Le minimum est de 1 et le maximum est de 60 secondes. La valeur par défaut est 20 secondes.
5. Vous pouvez également sélectionner l'option **Ignorer les erreurs de vérification**. Si cette option est sélectionnée, un certificat qui échoue à la vérification continue à être utilisé et une erreur est consignée. Si cette option n'est pas sélectionnée, aucun certificat dont la vérification échoue n'est utilisé.
6. Cliquez sur **Enregistrer**.

Portail de support client BlackBerry AtHoc

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

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

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

Commentaires sur la documentation

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

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

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

Informations juridiques

Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, 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, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

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

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

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada