BlackBerry Enterprise Identity

Administratorhandbuch

Inhalt

Was ist BlackBerry Enterprise Identity ?

BlackBerry Enterprise Identity ermöglicht die Authentifizierung für BlackBerry-Web-Apps wie die BlackBerry UEM Cloud-Verwaltungskonsole und BlackBerry Persona Mobile. BlackBerry Enterprise Identity bietet zudem Single Sign-On (SSO) für Cloud-Dienste, wie z. B. Microsoft Office 365, G Suite, BlackBerry Workspaces und viele andere. Bei der einmaligen Anmeldung (Single Sign-On) müssen Benutzer nicht mehrere Anmeldungen ausführen oder sich mehrere Kennwörter merken. Administratoren können außerdem benutzerdefinierte Dienste zu Enterprise Identity hinzufügen, um Benutzern Zugriff auf interne Anwendungen zu ermöglichen. Benutzer können von einem beliebigen Gerät aus auf die Dienste zugreifen, z. B. von iOS-, Android- oder BlackBerry 10-Geräten und sonstigen Rechnerplattformen.

Enterprise Identity ist in einem Bundle mit BlackBerry UEM und BlackBerry UEM Cloud enthalten. Administratoren nutzen die BlackBerry UEM- oder BlackBerry UEM Cloud-Konsole, um Dienste hinzuzufügen, Benutzer zu verwalten sowie zusätzliche Administratoren hinzuzufügen bzw. zu verwalten. Die Integration in BlackBerry-EMM-Produkte vereinfacht die Verwaltung von Benutzern und gewährt diesen Zugriff auf Cloud-Dienste über ihre Geräte.

Zur Verwendung von Enterprise Identity müssen Sie Benutzerlizenzen für die Collaboration Edition, die Application Edition oder die Content Edition von BlackBerry Enterprise Mobility Suite oder separate BlackBerry Enterprise Identity-Benutzerlizenzen erwerben. Weitere Informationen zu BlackBerry Enterprise Identity, einschließlich Informationen zum Erwerb von Enterprise Identity, finden Sie unter blackberry.com.

Die folgenden Browser werden für Administrationszwecke unterstützt: Internet Explorer 11, Google Chrome, Mozilla Firefox und Safari. Die Client-Verwendung wird unter allen zuvor genannten Browsern sowie nativen Browsern auf Geräten mit BlackBerry 10 OS Version 10.2.1 oder höher, iOS 8 oder höher und Android OS 4.0 oder höher unterstützt.

Funktion	Vorteil
Verbesserung der Mitarbeiterproduktivität	Mitarbeiter können ein Kennwort für alle Cloud-Dienste auf allen mobilen Geräten (iOS, Android und BlackBerry) sowie auf herkömmlichen Rechnerplattformen (Windows und macOS) verwenden. Auf diese Weise lässt sich der Aufwand mit mehreren Kennwörtern und Anmeldungen vermeiden.
Anpassen der Authentifizierung	Mit BlackBerry Enterprise Identity können Sie auf Grundlage Ihrer spezifischen Sicherheitsbedürfnisse die Authentifizierungsmethode für einen beliebigen Dienst, eine Benutzergruppe oder für eine Kombination aus beiden festlegen. Sie können sogar die Richtlinien Ihres Unternehmens bearbeiten, um diese an Situationen mit hohem Sicherheitsrisiko anzupassen.
Weiterentwicklung Ihrer mobilen Strategie	Benutzer und deren Identität sind für Enterprise Mobility-Lösungen äußerst wichtig. BlackBerry Enterprise Identity vereinheitlicht und vereinfacht den Zugriff auf Cloud-Dienste wie Microsoft Office 365, Salesforce, Google Apps, BlackBerry Workspaces oder die meisten SAML-basierten Apps und Dienste, welche die Produktivität Ihrer zunehmend mobilen Arbeitskräfte unterstützen.
Wirksamer Einsatz Ihrer EMM-Lösung von BlackBerry	Enterprise Identity ist vollständig in BlackBerry UEM integriert und bietet so branchenführende EMM-Lösungen mit besserer Kontrolle des Zugriffs auf alle Ihre Cloud-Dienste. Damit können Sie auf Funktionen wie das Aufrufen von Apps mit einmaligem Klick und SSO-Berechtigung, BlackBerry 2FA sowie mobiles Zero Sign-On (Mobile ZSO) zugreifen.

Erstmalige Verwendung von Enterprise Identity

BlackBerry UEM und BlackBerry UEM Cloud enthalten die BlackBerry Enterprise Identity Software. In BlackBerry UEM Version 12.7 MR1 und höher müssen Sie Enterprise Identity nicht aktivieren. Wenn Ihr Unternehmen über die entsprechenden Lizenzen verfügt, erfolgt die Aktivierung von Enterprise Identity automatisch.

Informationen zu Diensten, Berechtigungen und Gruppen

Dienste sind Anwendungen, die sich oft in der Cloud befinden und auf die Benutzer zugreifen müssen. Beispiele: Microsoft Office 365, BlackBerry Workspaces oder WebEx. Durch die Konfiguration eines Dienstes in BlackBerry UEM, BlackBerry UEM Cloud oder BlackBerry Enterprise Identity richten Sie eine sichere Schnittstelle zwischen Enterprise Identity und der Instanz oder dem Mandanten dieses Dienstes ein. Nachdem Sie mithilfe von BlackBerry UEM oder BlackBerry UEM Cloud einen Dienst hinzugefügt haben, können Sie die BlackBerry UEM-Verwaltungskonsole verwenden, um den Dienst zu verwalten und Benutzern Berechtigungen für den Dienst bereitzustellen.

Der effizienteste Weg, Benutzern Berechtigungen zuzuweisen, sind App-Gruppen. Eine App-Gruppe kann sowohl die SSO-Berechtigung für einen Dienst als auch für Client-Anwendungen umfassen, die Geräte benötigen, um mit dem Dienst interagieren zu können. Sie können Benutzern bzw. Benutzergruppen App-Gruppen zuweisen, sodass diese alles haben, um auf den Dienst zugreifen zu können.

Benutzergruppen bieten Administratoren die Möglichkeit, Berechtigungen für eine große Anzahl von Benutzern gleichzeitig zu verwalten, anstatt diese einzeln zuzuweisen bzw. wieder zu entfernen. Wenn ein Benutzer zu einer Gruppe hinzugefügt wird, wird diesem die Berechtigung automatisch zugewiesen. Somit kann dieser Benutzer sich auf einem beliebigen Gerät mit denselben Anmeldeinformationen bei einem bestimmten Dienst anmelden. Wenn ein Benutzer von einer Gruppe entfernt wird, verliert dieser automatisch die Zugriffsberechtigung für einen bestimmten Dienst. Dienstberechtigungen können, falls notwendig, auch einzelnen Benutzer zugewiesen werden.

Befristete Lizenzen	Beschreibung
Dienst	Dienste umfassen Workspaces, Box, Workday, WebEx, Salesforce und weitere, u a. auch benutzerdefinierte Dienste.
Berechtigung	Eine Berechtigung ist eine Zuweisung zu einem Dienst über BlackBerry UEM, die Enterprise Identity signalisiert, einem Benutzer oder einer Benutzergruppe Single Sign-On-Zugriff für einen bestimmten Dienst bereitzustellen.
App-Gruppe	Eine App-Gruppe ist eine Zusammenstellung von Apps, die Single Sign-On-Berechtigungen und die zugehörigen Binärdateien für Mobilgeräte umfassen können.
Benutzer	Ein Benutzer ist ein BlackBerry UEM-Benutzer.
Benutzergruppe	Eine Benutzergruppe ist eine Zusammenfassung von BlackBerry UEM-Benutzern.

Verwalten von Diensten

Wenn Sie BlackBerry UEM 12.7.x oder höher nutzen oder BlackBerry UEM Cloud, verwenden Sie die BlackBerry UEM-Verwaltungskonsole, um die Dienste Ihres Unternehmens zu verwalten.

Verwalten von Diensten in der BlackBerry UEM-Verwaltungskonsole

Bevor Sie in der BlackBerry UEM-Verwaltungskonsole SaaS oder andere Dienste konfigurieren können, muss der entsprechende Dienst von Ihrem Systemadministrator hinzugefügt werden. Weitere Informationen finden Sie unter Integrieren von Inhalten der SaaS-Dienste.

Nachdem Ihr Unternehmen die richtigen Lizenzen für BlackBerry Enterprise Identity erworben hat (weitere Informationen finden Sie im Lizenzierungsleitfaden für BlackBerry UEM), können Sie die BlackBerry UEM-Konsole für die Verwaltung der Dienste und ihrer Funktionen verwenden. Wenn ein Dienst hinzugefügt wird, müssen Sicherheits- und andere Parameter für Ihr Unternehmen festgelegt werden.

Nachdem Sie einen Dienst hinzugefügt haben, können Sie in der BlackBerry UEM-Verwaltungskonsole Benutzern Berechtigungen zuweisen, damit sie den Dienst auf Benutzerbasis oder über eine Gruppe verwenden können. Sie können die Konfiguration des Dienstes in der BlackBerry UEM-Verwaltungskonsole ändern.

Anzeigen einer Liste mit Dienstvorlagen in der BlackBerry UEM-Konsole

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity > Dienste**.
3. Klicken Sie auf +.

Eine Liste der verfügbaren Dienstvorlagen wird angezeigt.

Anzeigen einer Liste der benutzerdefinierten Dienste, die Sie in der BlackBerry UEM-Konsole erstellt haben

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity** > **Dienste**.

Die Liste mit den benutzerdefinierten Diensten wird angezeigt.

Erstellen eines SaaS-Dienstes in der BlackBerry UEM-Konsole

Hinweis: Wenn Sie zwei Instanzen desselben Diensttyps in BlackBerry UEM erstellen möchten (z. B. Box), müssen Sie für jede Instanz eine andere Entity-ID des Dienstanbieters angeben.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity > Dienste**.
3. Klicken Sie auf +.
4. Wählen Sie den Diensttyp aus, den Sie erstellen möchten (z. B. Box).
5. Geben Sie auf dem Bildschirm **BlackBerry Enterprise Identity-Dienst hinzufügen** die Metadaten zum Dienstanbieter ein. Diese Metadaten beziehen sich speziell auf den Dienstanbieter und Ihr Unternehmen. Beachten Sie, dass nur die mit der ausgewählten Dienstvorlage verknüpften Felder angezeigt werden.

Name	Beschreibung
Mobiles Zero Sign-On (ZSO)	Wählen Sie diese Option aus, wenn Sie das mobile Zero Sign-On aktivieren möchten.
Name	Geben Sie den Namen des SaaS-Anbieters ein.
Beschreibung	Die Mandantenbeschreibung ist optional.
Logo	Fügen Sie ein Logo hinzu, das mit dem Dienst verknüpft werden soll.
Entity-ID des Dienstanbieters	Geben Sie die URL oder einen eindeutigen Namen für den Zugriff auf den SaaS-Dienst ein.
Assertions-Verbraucherdienst (POST URL)	Geben Sie die vom Dienstanbieter bereitgestellte POST URL ein.
IdP-initiierte Anmeldeunterstützung	Geben Sie die Art der Anmeldeunterstützung ein, die Ihr Unternehmen benötigt.
Signaturoptionen	Geben Sie Ihre Assertion-Auswahl ein.
IdP-Signaturzertifikat	Geben Sie das mit dem Dienstanbieter gemeinsam genutzte x509-Zeritfikat ein.
Privater Schlüssel mit IdP-Signatur	Geben Sie den x509-Schlüssel für das entsprechende Signaturzertifikat ein. Bewahren Sie dieses sicher auf.
Verschlüsselungszertifikat	Geben Sie das Verschlüsselungszertifikat ein.
Dienstspezifische Informationen	Einige Dienste erfordern zusätzliche Information oder Informationen, die geringfügig von diesen Beschreibungen abweichen. Meistens sind diese Informationen jedoch bereits vorkonfiguriert.
Ansprüche – Attribut der Namenskennung	Wählen Sie das Attribut der Kennung für Ihren Anspruch auswählen.

Name	Beschreibung

SAML-Anspruchsattribute	• Name – Geben Sie einen SAML-Anspruchsnamen ein.
	• SAML-Attribut – Geben Sie Ihr SAML-Attribut ein.
	• SAML-Anspruchstyp
	  • Lokal – wenn Sie einen lokalen Anspruch auswählen, müssen Sie eine Option in der Attributwerteliste auswählen. Dadurch wird ein SAML-Attribut einem Attributtyp zugeordnet, der von BlackBerry Enterprise Identity erkannt wird, beispielsweise ein Benutzername.
	  • Statisch – wenn Sie einen statischen Anspruch auswählen, müssen Sie eine Option im Attributwertefeld eingeben.
	  • Verzeichnis: Wenn Sie Verzeichnis wählen, können Sie den Namen eines Active Directory-Attributs eingeben. Werte, die mit dem von Ihnen eingegebenen Text übereinstimmen, werden automatisch vorgeschlagen.
	• Attributwert – wählen Sie einen Attributwert aus oder geben Sie einen ein. Dies ist ein definierter Attributwert, den Ihr SaaS-Dienst gegebenenfalls benötigt, um den Dienst für die Benutzer Ihres Unternehmens einzurichten.
	• Attributtyp – wählen Sie einen Typ für das Attribut aus. Der Typ beruht auf Ihren SaaS-Dienstanforderungen. Der Standardtyp lautet „anyType“.
	• Wenn das Attribut erforderlich sein soll, aktivieren Sie optional das Kontrollkästchen **Erforderlich**.

6. Klicken Sie auf **Speichern**.

Hinzufügen eines ADFS-Anspruchsanbieter-Service

Wenn Ihr Unternehmen über Apps verfügt, die die formularbasierte Authentifizierung Active Directory Federation Services (ADFS) verwenden, können Sie einen ADFS-Anspruchsanbieter-Service hinzufügen, damit Enterprise Identity die Authentifizierung der ADFS-Apps mithilfe eines formularbasierten Authentifizierungstyps ausführen kann.

Enterprise Identity unterstützt ADFS 2019 und höher

Bevor Sie beginnen:

- Stellen Sie sicher, dass die ADFS-Rolle dem Active Directory-Server hinzugefügt wurde.
- Stellen Sie sicher, dass UEM mit dem Active Directory-Server verbunden ist, der die ADFS-Rolle aufweist.

1. Klicken Sie in der UEM-Verwaltungskonsole auf **Einstellungen** > **BlackBerry Enterprise Identity** > **Dienste**.
2. Klicken Sie in der Tabelle **SAML-Dienste** auf +.
3. Klicken Sie auf **ADFS-Anspruchsanbieter**.
4. Wenn Sie ZSO für Benutzer aktivieren möchten, aktivieren Sie die Kontrollkästchen **Mobile ZSO zulassen, wenn durch Authentifizierungsrichtlinie festgelegt** und **Kerberos Desktop ZSO zulassen, wenn durch die Authentifizierungsrichtlinie festgelegt**.
5. Geben Sie einen Namen und eine Beschreibung für den Dienst ein.
6. Geben Sie in das Feld **Entity-ID des Dienstanbieters** `http://<adfs_host>/adfs/services/trust` ein, wobei *adfs_endpoint* der Name des Active Directory-Servers mit der ADFS-Rolle ist.
7. Geben Sie in das Feld **Assertions-Verbraucherdienst (POST URL)** `http://<adfs_host>/adfs/services/ls` ein, wobei *adfs_endpoint* der Name des Active Directory-Servers mit der ADFS-Rolle ist.

8. Geben Sie in das Feld **URL des Einzelabmeldungsdiensts** `http://<adfs_host>/adfs/services/trust` ein, wobei *adfs_endpoint* der Name des Active Directory-Servers mit der ADFS-Rolle ist.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Weisen Sie den Dienst Benutzern zu.

Konfigurieren des Anspruchsanbieters in ADFS

Bevor Sie beginnen: Hinzufügen eines ADFS-Anspruchsanbieter-Service

1. Klicken Sie in der UEM-Verwaltungskonsole auf **Einstellungen** > **BlackBerry Enterprise Identity** > **Dienste**.
2. Klicken Sie in der Tabelle **SAML-Dienste** auf den ADFS-Dienst „Anspruchsanbieter“.
3. Klicken Sie im Abschnitt **SAML-Dienst-Metadaten** auf den Link zum Herunterladen der SAML-Dienst-Metadaten. Kopieren Sie die Datei auf den Windows-Server, auf dem ADFS ausgeführt wird.
4. Öffnen Sie den ADFS-Manager.
5. Klicken Sie im linken Fensterbereich auf **Anspruchsanbieter-Vertrauensstellungen**.
6. Klicken Sie im rechten Fensterbereich auf **Anspruchsanbieter hinzufügen**.
7. Klicken Sie im **Assistenten für Anspruchsanbieter-Vertrauensstellungen** auf **Start** > **Weiter**.
8. Wählen Sie **Daten über den Anspruchsanbieter aus der Datei importieren** aus, und öffnen Sie die Metadatendatei, die Sie in Schritt 3 heruntergeladen haben. Klicken Sie auf **Weiter**.
9. Geben Sie einen Namen und eine Beschreibung für die Anspruchsanbieter-Vertrauensstellung ein. Klicken Sie auf **Hinzufügen**, bis die Schaltfläche „Speichern“ angezeigt wird.
10. Klicken Sie auf **Speichern**.

Wenn Sie Ihre ADFS-Konfiguration testen möchten, können Sie eine Test-App mit Claims X-Ray erstellen. Weitere Informationen finden Sie unter https://adfshelp.microsoft.com/ClaimsXray/TokenRequest.

Verwenden von Enterprise Identity als Standard-Anspruchsanbieter

Um Enterprise Identity als Standard-Anspruchsanbieter zu verwenden, können Sie den folgenden Befehl in Windows PowerShell ausführen. Wenn Enterprise Identity der Standard-Anspruchsanbieter ist, werden Benutzer beim Zugriff auf einen Dienst nicht zur Authentifizierung aufgefordert.

Führen Sie in Windows PowerShell den folgenden Befehl aus:

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

Beispiel: Konfigurieren von Anspruchszuordnungen für Office 365

Die folgenden Schritte sind ein Beispiel für die Konfiguration der grundlegenden Anspruchszuordnung für Microsoft Office 365. In Ihrer Organisation gelten möglicherweise andere Anforderungen für die Anspruchszuordnung.

Bevor Sie beginnen: Verwenden von Enterprise Identity als Standard-Anspruchsanbieter.

1. Klicken Sie im AD FS Manager auf **Anspruchsregeln bearbeiten** für den von Ihnen konfigurierten Enterprise Identity Anspruchsanbieter.
2. Klicken Sie auf **Regel hinzufügen** > **Ansprüche mithilfe einer benutzerdefinierten Regel senden**.
3. Wählen Sie im Vorlagenfenster **Regel auswählen** in der Dropdown-Liste **Vorlage für Anspruchsregel** die Option **Ansprüche mithilfe einer benutzerdefinierten Regel senden**. Klicken Sie auf **Weiter**.
4. Geben Sie im Fenster **Regel konfigurieren** im Feld **Name der Anspruchsregel** die Wortfolge `Pass all claims` ein.

5. Geben Sie im Fensterbereich **Benutzerdefinierte Regel** Folgendes ein:

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

6. Klicken Sie auf **Fertigstellen**.
7. Geben Sie im Fenster **Regel konfigurieren** im Feld **Name der Anspruchsregel** die Wortfolge `Transform UPN` ein.
8. Geben Sie im Fensterbereich **Benutzerdefinierte Regel** Folgendes ein:

```
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,
 "^(?<Benutzer>.*)$", "${user}<Domänensuffix für Ihren Benutzer>"), ValueType =
 c.ValueType);
```

   Wobei das Domänensuffix die E-Mail-Domäne für Benutzer ist (z. B. „${user}@example.com“).
9. Klicken Sie auf **Fertigstellen**.
10. Klicken Sie in der UEM-Verwaltungskonsole auf **Einstellungen** > **BlackBerry Enterprise Identity** > **Dienste**.
11. Klicken Sie in der Tabelle **SAML-Dienste** auf den von Ihnen erstellten ADFS-Dienst.
12. Wählen Sie unter **Ansprüche** in der Dropdown-Liste **Attribut der Namenskennung** die Option **Unveränderliche ID** aus.
13. Klicken Sie in der Tabelle „SAML-Anspruchsattribute“ auf +. Gehen Sie wie folgt vor:
    a) Geben Sie `Username` im Feld „Name“ ein.
    b) Wählen Sie unter „SAML-Attribut“ die Option „http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name“ aus.
    c) Legen Sie den SAML-Anspruchstyp auf „Lokal“ fest.
    d) Setzen Sie den Attributwert auf den Namen, den Sie für das Anspruchsattribut eingegeben haben (z. B. Benutzername).
    e) Legen Sie den Attributwert auf „anyType“ fest.
    f) Klicken Sie auf **Speichern**.
14. Klicken Sie in der Tabelle „SAML-Anspruchsattribute“ auf +. Gehen Sie wie folgt vor:
    a) Geben Sie `UPN` im Feld „Name“ ein.
    b) Wählen Sie unter „SAML-Attribut“ die Option „http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn“ aus.
    c) Legen Sie den SAML-Anspruchstyp auf „Lokal“ fest.
    d) Setzen Sie den Attributwert auf den Namen, den Sie für das Anspruchsattribut eingegeben haben (z. B UPN).
    e) Legen Sie den Attributwert auf „anyType“ fest.
    f) Klicken Sie auf **Speichern**.
15. Klicken Sie in der Tabelle „SAML-Anspruchsattribute“ auf +. Gehen Sie wie folgt vor:
    a) Geben Sie `ImmutableID` im Feld „Name“ ein.
    b) Wählen Sie unter „SAML-Attribut“ die Option „http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID“ aus.
    c) Legen Sie den SAML-Anspruchstyp auf „Lokal“ fest.
    d) Setzen Sie den Attributwert auf den Namen, den Sie für das Anspruchsattribut eingegeben haben (z. B ImmutableID).
    e) Legen Sie den Attributwert auf „anyType“ fest.

16. Klicken Sie auf **Speichern**.

Hinzufügen eines benutzerdefinierten Dienstes in der BlackBerry UEM-Konsole

BlackBerry bietet eine zunehmende Auswahl vordefinierter Dienstvorlagen. Als Administrator haben Sie zudem die Möglichkeit, benutzerdefinierte Dienste zu BlackBerry Enterprise Identity hinzuzufügen. Die meisten Dienste, die SAML 2.0-Protokolle verwenden, können integriert werden. Die von Ihnen integrierten SAML-Dienste können speziell auf Ihr Unternehmen zugeschnitten sein, oder Sie können einen Dienst eines SaaS-Anbieters auswählen, der für den breiteren Einsatz geeignet ist.

Wenn ein Dienst aktiviert wurde, können berechtigte Benutzer diesen verwenden. Wenn ein Dienst deaktiviert wurde, können berechtigte Benutzer nicht mehr darauf zugreifen, bis er wieder aktiviert wird.

Detaillierte Informationen zu den verfügbaren Dienstvorlagen finden Sie unter Integrieren von SaaS-Diensten.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity > Dienste**.
3. Klicken Sie auf +.
4. Wählen Sie **Benutzerdefinierter Dienst** aus.
5. Füllen Sie die Felder zum Konfigurieren des benutzerdefinierten Dienstes aus.
   - Wenn Sie bei Auswahl eines lokalen Anspruchs einen SAML-Anspruch hinzufügen, müssen Sie anschließend eine Option in der Attributwerteliste auswählen. Dadurch wird ein SAML-Attribut einem Attributtyp zuordnet, der von BlackBerry Enterprise Identity erkannt wird, beispielsweise ein Benutzername.
   - Wenn Sie bei Auswahl eines statischen Anspruchs einen SAML-Anspruch hinzufügen, müssen Sie anschließend eine Option in der Attributwerteliste eingeben.
6. Klicken Sie auf **Speichern**.

Ändern eines aktiven Dienstes in der BlackBerry UEM-Konsole

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity > Dienste**.
3. Klicken Sie auf den Dienst, den Sie ändern möchten.
4. Füllen Sie zum Ändern der Konfiguration eines Dienstes oder einer Funktion, die bearbeitet werden kann, die Felder im Bereich **Dienstkonfiguration** aus. Einige Dienste lassen keine Änderungen zu.
5. Klicken Sie auf **Speichern**.

Entfernen eines Dienstes von der BlackBerry UEM-Konsole

Bevor Sie einen Dienst entfernen, müssen Sie in der BlackBerry UEM-Verwaltungskonsole alle Benutzerberechtigungen von diesem Dienst entfernen.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity > Dienste**.
3. Klicken Sie auf das X neben dem zu löschenden Dienst.
4. Klicken Sie auf **Entfernen**.

Anzeigen von SAML-Konfigurationseinstellungen in der BlackBerry UEM-Konsole

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity > Dienste**.
3. Klicken Sie auf die SaaS-Dienstkonfiguration, um die SAML-Einstellungen anzuzeigen.

Exportieren von SAML-Dienst-Metadaten in der BlackBerry UEM-Konsole

Sie benötigen die SAML-Dienst-Metadaten gegebenenfalls, um eine sichere Schnittstelle zwischen BlackBerry Enterprise Identity und Ihrer Instanz oder Ihrem Mandanten des Dienstes einzurichten, den Sie konfigurieren (beispielsweise Box).

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity > Dienste**.
3. Klicken Sie auf die SaaS-Dienstkonfiguration, um die Kopfzeile der SAML-Metadaten anzuzeigen.
4. Klicken Sie auf den Hyperlink, um die XML-Datei herunterzuladen.

Hinzufügen einer OpenID Connect-App

Sie können OpenID Connect-Apps hinzufügen, die Ihrem Unternehmen oder einem UEM-Mandanten zur Verfügung gestellt wurden. OpenID Connect-Apps werden von einem Administrator oder App-Entwickler zur Verfügung gestellt.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity** > **Dienste**.
3. Klicken Sie in der Tabelle **OpenID Connect-Apps** auf +.
   Eine Liste der verfügbaren OpenID Connect-Apps wird angezeigt.
4. Wählen Sie eine App aus.
5. Führen Sie auf dem Bildschirm **BlackBerry Enterprise Identity-Dienst hinzufügen** eine der folgenden Aktionen aus:
   - Aktivieren Sie **Mobile ZSO zulassen, wenn durch Authentifizierungsrichtlinie festgelegt**.
   - Aktivieren Sie **Kerberos-Authentifizierung für Desktop ZSO zulassen, wenn durch Authentifizierungsrichtlinie festgelegt**.
6. Überprüfen Sie die Bereiche für die App. Klicken Sie auf **Speichern**.

Um die App zu bearbeiten, klicken Sie auf den App-Namen in der Tabelle „OpenID Connect-Apps“.

Zustimmung für eine OpenID Connect-App aktualisieren

Wenn die für eine OpenID Connect-App-Änderung erforderlichen Berechtigungsbereiche vorhanden sind, müssen Sie die Zustimmung für die App aktualisieren. Wenn sich die erforderlichen Bereiche ändern, wird eine Benachrichtigung im Abschnitt OpenID Connect der Seite BlackBerry Enterprise Identity Services angezeigt.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity** > **Dienste**.
3. Klicken Sie in der Tabelle der **OpenID Connect**-Apps im Abschnitt **Zustimmung erforderlich** auf die Benachrichtigung für eine App.
4. Überprüfen Sie im Dialogfeld **App aktualisieren** die Bereiche oder Clients, die hinzugefügt oder entfernt wurden. Klicken Sie auf **Speichern**.

Entfernen einer OpenID Connect-App

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen**.
2. Klicken Sie auf **BlackBerry Enterprise Identity** > **Dienste**.
3. Klicken Sie in der Tabelle **OpenID Connect-Apps** auf ✕ neben der App, die Sie entfernen möchten.
4. Klicken Sie im Dialogfeld **Zustimmung entfernen** auf **Entfernen**.

Anmelden bei der BlackBerry Enterprise Identity-Konsole

Um verschiedene Aufgaben, wie das Anzeigen von Systemprotokollen, durchzuführen, müssen Sie sich bei der BlackBerry Enterprise Identity-Konsole anmelden.

Bevor Sie beginnen: Aktivieren Sie Popups in Ihrem Browser.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**.
2. Klicken Sie auf **Enterprise Identity**. In einer Meldung wird die Abfrage angezeigt, ob Sie die Enterprise Identity-Services synchronisieren möchten.
3. Klicken Sie auf **Enterprise Identity-Konsole öffnen**. Die Administratorkonsole wird in einer neuen Browserregisterkarte geöffnet. Falls die Konsole nicht geöffnet wird, stellen Sie sicher, dass Sie die Pop-ups in Ihrem Browser aktiviert haben.
4. Schließen Sie die Browserregisterkarte, wenn Sie fertig sind.

Verwalten von Authentifizierungsebenen

In Enterprise Identity sind drei Authentifizierungstypen verfügbar. Die Rangfolge dieser Authentifikatoren kann in der BlackBerry UEM-Konsole auf der Seite **Einstellungen** geändert werden. Weitere Informationen zur Rangordnung finden Sie unter Enterprise Identity-Einstellungen anpassen.

Authentifikatortyp	Beschreibung
Unternehmenskennwort	Diese Sicherheitsmethode erfordert eine Kennworteingabe, bevor Benutzer auf einen Dienst zugreifen können. Hierbei handelt es sich um die Standardmethode. Dieses Kennwort ist derzeit mit einem Benutzerkonto in Active Directory, einem LDAP-Verzeichnis oder BlackBerry UEM verknüpft.
Enterprise-Kennwort und BlackBerry 2FA	Diese Sicherheitsmethode nutzt BlackBerry 2FA und erfordert sowohl ein Kennwort als auch die Bestätigung auf dem Mobilgerät eines Benutzers, bevor dieser auf einen Dienst zugreifen kann.
Mobile ZSO	Diese auf Mobilgeräten verfügbare Sicherheitsmethode ermöglicht es Benutzern, ohne explizite Authentifizierung auf einen Dienst zuzugreifen. Stattdessen wird die Authentifizierung des Benutzers mit dem Gerät oder Sicherheitscontainer als Identitätsnachweis verwendet.
Ping-Kennwort	Bei dieser für PingFederate-Benutzer verfügbaren Sicherheitsmethode müssen Benutzer ihr Ping Identity-Kennwort eingeben, bevor sie auf einen Dienst zugreifen können. Für zusätzliche Sicherheit können Sie auch die Bestätigung einer Eingabeaufforderung oder die Eingabe der PingID von Benutzern anfordern.

Sie können diese Authentifizierungsrichtlinien einem Benutzer bzw. einer Benutzergruppe für jeden Dienst zuweisen, indem Sie eine Authentifizierungsrichtlinie definieren. Weitere Informationen über Richtlinien finden Sie unter Verwalten von Authentifizierungsrichtlinien.

Aktivieren der Zwei-Faktor-Authentifizierung

Die Aktivierung der Zwei-Faktor-Authentifizierung entspricht der Aktivierung von BlackBerry 2FA, der Festlegung der Authentifikatorrangfolge und der Zuweisung einer Authentifizierungsrichtlinie, für die die entsprechende Authentifizierungsebene benötigt wird.

Bevor Sie beginnen:

- Aktivieren Sie BlackBerry 2FA in BlackBerry UEM, und wenden Sie das BlackBerry 2FA-Profil auf den Benutzer oder die Gruppe an.
- Stellen Sie sicher, dass alle Benutzer, die BlackBerry 2FA verwenden müssen, über ihre Mobilgeräte verfügen und diese aktiviert sind. Weitere Informationen zum Aktivieren von Geräten finden Sie in der Dokumentation für BlackBerry 2FA.

1. Weisen Sie BlackBerry 2FA einer Authentifizierungsebene zu. Weitere Informationen finden Sie unter Verwalten von Authentifizierungsebenen.
2. Konfigurieren Sie eine Authentifizierungsrichtlinie, die BlackBerry 2FA als zu verwendende Authentifizierungsebene festlegt, welche von einer bestimmten Benutzergruppe oder einem bestimmten Dienst genutzt wird. Weitere Informationen finden Sie unter Verwalten von Authentifizierungsrichtlinien.

Aktivieren von Mobile ZSO

Wenn Sie die Funktion des mobilen Zero Sign-On (Mobile ZSO) aktivieren, wird diese für Dienste aktiviert, die Sie nutzen möchten. Dabei legen Sie eine Authentifikatorrangfolge fest und weisen eine Authentifizierungsrichtlinie zu, die eine Authentifizierungsebene benötigt.

Wenn Mobile ZSO für einen Dienst aktiviert wird, kann dieser Dienst die Authentifizierung mit dem Zertifikat auf dem verwalteten Gerät eines Benutzers durchführen, ohne einen Benutzernamen oder ein Kennwort zu verwenden.

Aktivieren von Mobile ZSO in BlackBerry UEM

Bevor Sie beginnen:

- Benutzer benötigen ein Android Enterprise-Gerät mit einem geschäftlichen Profil, ein Samsung Knox-, iOS- oder BlackBerry 10-Gerät.
- Benutzer benötigen BlackBerry Secure Connect Plus auf ihren Geräten.

1. Melden Sie sich bei BlackBerry UEM als Administrator an.
2. Klicken Sie in der Menüleiste auf **Einstellungen > BlackBerry Enterprise Identity > Dienste.**
3. Klicken Sie auf den Dienst, für den Sie Mobile ZSO aktivieren möchten.
4. Wählen Sie die Option **Mobile ZSO zulassen, wenn durch Authentifizierungsrichtlinie festgelegt**.
5. Klicken Sie auf **Speichern**.
6. Ordnen Sie mobiles Zero Sign-On einer Authentifizierungsebene zu. Weitere Informationen finden Sie unter Verwalten von Authentifizierungsebenen.
7. Konfigurieren Sie eine Authentifizierungsrichtlinie, die mobiles Zero Sign-On als zu verwendende Authentifizierungsebene festlegt, welche von einer bestimmten Benutzergruppe oder einem bestimmten Dienst genutzt wird. Weitere Informationen finden Sie unter Verwalten von Authentifizierungsrichtlinien.

Wenn mobiles Zero Sign-On (Mobile ZSO) für einen Dienst aktiviert wurde, können sich Benutzer über mobiles Zero Sign-On für einen Dienst authentifizieren. Die in BlackBerry UEM zugewiesene allgemeine Authentifizierungsrichtlinie muss die Verwendung von mobilem Zero Sign-On zulassen.

Wenn Sie einen Dienst für Mobile ZSO ohne Fallback-Authentifikator konfigurieren, kann auf diesen Dienst nur von verwalteten Mobilgeräten aus zugegriffen werden. Falls jedoch ein Fallback-Authentifikator mit Kennwort konfiguriert wird, wird Mobile ZSO auf verwalteten Mobilgeräten verwendet, und der Benutzer erhält die Erlaubnis, das Kennwort auch auf anderen Geräten zu nutzen.

Verwalten von Risikofaktoren

Risikofaktoren stellen optionale Funktionen in Authentifizierungsrichtlinien dar, die eine Möglichkeit bieten, die Authentifizierungsebene basierend auf dem Risiko abzustimmen. Wenn Benutzer einen vertrauenswürdigen Browser oder Netzwerk verwenden, können sie leichter auf benötigte Dienste zugreifen. In anderen Fällen kann jedoch eine strengere Authentifizierungsrichtlinie angewandt werden.

Risikofaktor	Beschreibung
Browsererkennung	Durch diesen Risikofaktor werden Benutzer aufgefordert, beim erstmaligen Öffnen eines Browsers einen vertrauenswürdigen Verweis zwischen Browser und Enterprise Identity einzurichten. Nach dem Einrichten des vertrauenswürdigen Verweises kann bei späteren Anmeldungen eine einfachere Authentifizierungsebene verwendet werden. Die Benutzer können Einträge zu vertrauenswürdigen Browsern in BlackBerry UEM Self-Service anzeigen und entfernen.
Netzwerkerkennung	Mit diesem Risikofaktor wird geprüft, ob die App oder der Browser von Benutzern mit demselben Netzwerk wie der BlackBerry UEM-Server verbunden ist. Ist dies nicht der Fall, kann eine höhere Authentifizierungsebene verwendet werden. Mit diesem Risikofaktor kann Benutzern eine leichtere Anmeldung bei bestimmten Diensten ermöglicht werden, wenn sie das geschäftliche Netzwerk verwenden. Weitere Informationen zur Konfiguration dieses Risikofaktors finden Sie unter Konfigurieren des Risikofaktors der Netzwerkerkennung. Wenn Sie die Netzwerkerkennung global deaktivieren möchten, können Sie sich bei der Enterprise Identity-Konsole anmelden, und die Erkennung geschäftlicher Netzwerke in der UEM-Mandantenliste ausschalten. **Hinweis:** Sie können den Risikofaktor der Netzwerkerkennung in BlackBerry UEM Cloud nicht aktivieren.

Konfigurieren des Risikofaktors der Netzwerkerkennung

Bevor Sie beginnen: Sie können den Risikofaktor der Netzwerkerkennung nicht in BlackBerry UEM Cloud aktivieren.

1. Klicken Sie in der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > BlackBerry Enterprise Identity > Einstellungen**.
2. Geben Sie den Namen des geschäftlichen Netzwerk-Hosts des BlackBerry UEM-Servers ein, den Ihre geschäftlichen Computer und Geräte verwenden. Geben Sie alternativ dazu den DNS-Poolnamen ein, der in mehrere IP-Adressen des BlackBerry UEM-Servers aufgelöst wird.
3. Bestätigen Sie, dass Ihre geschäftlichen Computer und Geräte über die aufgeführte Portnummer eine Verbindung zum Hostnamen aufbauen können. Der Risikofaktor funktioniert nicht, wenn der Port durch eine Firewall gesperrt wird.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Einstellungen** > **Infrastruktur** > **Serverzertifikate** > **SSL-Zertifikat für BlackBerry Web Services**.

   Die Browser und Geräte des geschäftlichen Computers müssen das Zertifikat als vertrauenswürdig akzeptieren, wenn sie eine Verbindung zum Hostnamen des geschäftlichen Netzwerks herstellen, und bei dem

Standardzertifikat handelt es sich um ein selbstsigniertes, nicht vertrauenswürdiges Zertifikat. Sie können ein vertrauenswürdiges BlackBerry Web Services-Zertifikat in BlackBerry UEM hochladen.

Wenn Sie fertig sind: Bei einigen Webbrowsern ist möglicherweise ein externes vertrauenswürdiges Zertifikat erforderlich. Falls dies der Fall ist, können Sie ein neues BlackBerry Web Services-Zertifikat in BlackBerry UEM hochladen. Klicken Sie auf **Einstellungen** > **Infrastruktur** > **Serverzertifikate** > **SSL-Zertifikat für BlackBerry Web Services**.

Wenn Sie fertig sind: Wenn Sie eine Enterprise-Identity-Authentifizierungsrichtlinie erstellen oder bearbeiten, klicken Sie auf das Kontrollkästchen **Netzwerkerkennung**, um den Risikofaktor hinzuzufügen. Weitere Informationen zur Erstellung von Authentifizierungsrichtlinien finden Sie unter Erstellen einer Enterprise Identity-Authentifizierungsrichtlinie.

Verwalten von Authentifizierungsrichtlinien

Die BlackBerry UEM-Verwaltungskonsole wird verwendet, um Authentifizierungsrichtlinien zu erstellen, zu verwalten und deren Rangfolge festzulegen. Richtlinien können pro Dienst aufgehoben werden. Allgemeine Informationen zu Richtlinien und Profilen finden Sie unter IT-Richtlinien in der BlackBerry UEM-Dokumentation für Administratoren.

Erstellen einer Enterprise Identity-Authentifizierungsrichtlinie

Führen Sie die folgenden Schritte zum Erstellen einer Enterprise Identity-Richtlinie für Benutzergruppen aus.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Konsole auf **Richtlinien und Profile** > **BlackBerry Enterprise Identity**.
2. Klicken Sie auf das + neben **Authentifizierungsrichtlinien**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Legen Sie in der Dropdown-Liste **Mindestauthentifizierungsebene** eine Authentifizierungsebene fest. Weitere Informationen finden Sie unter Verwalten von Authentifizierungsebenen.
5. Klicken Sie in der Tabelle **Risikoszenarien** auf das +.
6. Geben Sie einen Namen und eine Beschreibung ein.
7. Wählen Sie in der Dropdown-Liste **Mindestauthentifizierungsebene** die gewünschte Authentifizierungsebene, die angewendet werden soll, wenn die Risikofaktoren erfüllt sind.
8. Wählen Sie in der Liste **Risikofaktorkombination** eine der folgenden Optionen aus:
   - Wenn Sie alle ausgewählten Risikofaktoren auf das Szenario anwenden möchten, wählen Sie die Option **Alle ausgewählten Faktoren sind vorhanden**.
   - Wenn Sie beliebige der ausgewählten Risikofaktoren für das Szenario verwenden möchten, wählen Sie die Option **Beliebige der ausgewählten Faktoren sind vorhanden** aus.
9. Wenn Sie herausfinden möchten, ob die App oder der Browser eines Benutzers mit demselben Netzwerk wie der BlackBerry UEM-Server verbunden ist, wählen Sie die Option **Netzwerkerkennung**, und wählen Sie in der Dropdown-Liste **Konfiguration** die gewünschte Option aus. Beachten Sie, dass Sie den Risikofaktor „Netzwerkerkennung“ in BlackBerry UEM Cloud nicht aktivieren können.
10. Wenn Sie eine Vertrauensreferenz zwischen dem Browser und Enterprise Identity beim ersten Öffnen eines Browsers herstellen möchten, wählen Sie die Option **Browser-Erkennung**, und wählen Sie in der Dropdown-Liste **Konfiguration** die gewünschte Option aus.
11. Wenn Sie Risikoebenen und Geozonen von BlackBerry Persona Mobile als Risikofaktoren verwenden möchten, wählen Sie die Option **BlackBerry Persona** aus, und aktivieren Sie dann eine der folgenden Optionen:
    - **Verhaltensrisikostufe**: BlackBerry Persona Cloud-Services in der BlackBerry Infrastructure erfassen und verarbeiten App-Daten und verwenden diese zur Berechnung der Risikostufe des jeweiligen Benutzers.
    - **Vom Administrator definierte Geozone**: Wählen Sie eine Geozone aus, die der BlackBerry UEM-Administrator Ihres Unternehmens erstellt hat.

      Hinweis: Weitere Informationen zu Risikostufen und Geozonen finden Sie in der BlackBerry Persona Mobile-Dokumentation.
    - **Risikostufe der Geozone**: Wählen Sie zwischen „Hoch“, „Mittel“ oder „Niedrig“. Diese Einstellung gibt eine Risikostufe an, die einem Benutzer zugeordnet werden kann, indem der physische Standort des Benutzers mit der Region verglichen wird, die in einer vom Administrator definierten Geozone oder einer gelernten Geozone enthalten ist.
12. Klicken Sie auf **Speichern**.

13. Wenn Sie eine Ausnahme für einen der Dienste Ihres Unternehmens erstellen möchten, klicken Sie auf **Dienstausnahmen verwalten**, wählen Sie den Dienst aus der Liste, und richten Sie alle erforderlichen Risikoszenarien für den Dienst ein.
14. Wiederholen Sie ggf. die Schritte 5 bis 11, um weitere Risikoszenarien hinzuzufügen. Beachten Sie, dass für jedes Risikoszenario eine eindeutige Reihe von Risikofaktoren verwendet werden muss.
15. Klicken Sie auf **Speichern**.

Zuweisen einer Enterprise Identity-Richtlinie zu einer Benutzergruppe

Bevor Sie beginnen: Erstellen Sie eine Enterprise Identity-Richtlinie..

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Gruppen** > **Benutzer**.
2. Erstellen Sie entweder eine neue Gruppe, oder klicken Sie auf den Namen der Gruppe, die Sie bearbeiten möchten.
3. Klicken Sie auf die Registerkarte **BlackBerry Enterprise Identity**.
4. Klicken Sie auf +.
5. Wählen Sie aus der Dropdown-Liste eine Authentifizierungsrichtlinie aus.
6. Klicken Sie auf **Zuweisen**.

Löschen einer Enterprise Identity-Richtlinie

Bevor Sie beginnen: Erstellen eines Enterprise Identity-Profils.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Richtlinien und Profile** > **BlackBerry Enterprise Identity**.
2. Klicken Sie auf den Namen des Profils, das Sie löschen möchten.
3. Klicken Sie auf das .
4. Klicken Sie auf **OK**.

Verwenden von Authentifikatorebenen-Rangordnungen und Authentifizierungsrichtlinien zur Verwaltung der Sicherheit

Sie können die Authentifikatorebenen-Rangordnung und BlackBerry Enterprise Identity-Authentifizierungsrichtlinien verwenden, um die Authentifizierungstypen anzugeben, die Benutzer bei der Anmeldung bei einem Dienst durchführen müssen. Die Authentifikatorrangfolgen sind Sicherheitsmethoden, die festlegen, welche Art von Benutzerauthentifizierung bei der Dienstanmeldung erforderlich ist. Sie verwenden Risikoszenarien und Risikofaktoren in Authentifizierungsrichtlinien, um die Einstellungen festzulegen, die für Benutzer und Gruppen gelten, wenn sie auf Enterprise Identity-Dienste zugreifen.

Zusätzliche Authentifizierung erforderlich, wenn Benutzer mit einem externen Netzwerk verbunden sind

Führen Sie die folgenden Schritte aus, damit Benutzer ihr Kennwort eingeben müssen und auf eine BlackBerry 2FA-Aufforderung reagieren müssen, wenn sie versuchen, über ein externes Netzwerk eine Verbindung zu einem Dienst herzustellen. Sie können auch zulassen, dass sich Benutzer nur mit ihrem Kennwort von einem beliebigen Netzwerk aus authentifizieren. **Hinweis:** Sie können den Risikofaktor Netzwerkerkennung in BlackBerry UEM Cloud nicht aktivieren.

Authentifikatorrangfolge festlegen

1. Klicken Sie in der Menüleiste auf **Einstellungen > BlackBerry Enterprise Identity > Einstellungen**.
2. Setzen Sie im Abschnitt **Authentifikatorebenen-Rangordnung** das **Enterprise-Kennwort** auf Ebene 1 und **Enterprise-Kennwort + BlackBerry 2FA** auf Ebene 3. Weitere Informationen zum Einrichten von BlackBerry 2FA finden Sie unter Zwei-Faktor-Authentifizierung aktivieren.
3. Klicken Sie auf **Speichern**.

Hinzufügen einer Authentifizierungsrichtlinie für externe Netzwerke

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**. Klicken Sie unter „Verwaltete Geräte“ auf **BlackBerry Enterprise Identity**.
2. Klicken Sie im Bereich **Authentifizierungsrichtlinien** auf **Richtlinie hinzufügen**.
3. Geben Sie einen Namen und eine Beschreibung für die Authentifizierungsrichtlinie ein.
4. Wählen Sie in der Dropdown-Liste **Mindestauthentifizierungsebene** Ebene 1.

   Diese Ebene entspricht der Enterprise-Kennwort-Authentifikatorrangfolge, die Sie in der vorherigen Aufgabe festgelegt haben. Wenn Sie diese Richtlinie speichern, ohne ein Risikoszenario hinzuzufügen und es Benutzern zuzuweisen, müssen diese bei der Anmeldung bei einem Dienst nur ihr Enterprise-Kennwort eingeben. Wenn Sie eine zusätzliche Authentifizierung basierend auf dem Netzwerktyp verlangen möchten, mit dem sie verbunden sind, führen Sie die folgenden Schritte durch, um ein Risikoszenario hinzuzufügen.
5. Klicken Sie in der Tabelle **Risikoszenarien** auf +.
6. Geben Sie einen Namenund eine Beschreibung für das Szenario ein.
7. Wählen Sie in der Dropdown-Liste **Mindestauthentifizierungsebene** Ebene 3. Diese Ebene entspricht der Enterprise-Kennwort- und BlackBerry 2FA-Authentifikatorrangfolge, die Sie in der vorherigen Aufgabe festgelegt haben.
8. Klicken Sie auf **Netzwerkerkennung**.

9. Wählen Sie in der Dropdown-Liste **Konfiguration** die Option **Nicht in einem Geschäftsnetzwerk**.

   Wenn Sie diese Option konfigurieren und einer der Benutzer Ihres Unternehmens sich nicht in einem Geschäftsnetzwerkbefindet und versucht, sich bei einem Dienst anzumelden, muss er sein Enterprise-Kennwort eingeben und auf eine BlackBerry 2FA-Aufforderung auf seinem Gerät reagieren.
10. Klicken Sie auf **Speichern**.
11. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Weisen Sie die Authentifizierungsrichtlinie Benutzern oder Gruppen zu.

Zusätzliche Authentifizierung bei erstmaliger Verwendung des Browsers anfordern

Führen Sie die folgenden Schritte aus, damit Benutzer ihr Kennwort eingeben und auf eine BlackBerry 2FA-Aufforderung reagieren müssen, wenn sie versuchen, über einen Browser erstmalig eine Verbindung zu einem Dienst herzustellen. Nach dem Einrichten des vertrauenswürdigen Verweises kann bei späteren Anmeldungen eine einfachere Authentifizierungsebene verwendet werden.

Authentifikatorrangfolge festlegen

1. Klicken Sie in der Menüleiste auf **Einstellungen > BlackBerry Enterprise Identity > Einstellungen**.
2. Setzen Sie im Abschnitt **Authentifikatorebenen-Rangordnung** das **Enterprise-Kennwort** auf Ebene 1 und **Enterprise-Kennwort + BlackBerry 2FA** auf Ebene 3. Weitere Informationen zum Einrichten von BlackBerry 2FA finden Sie unter Zwei-Faktor-Authentifizierung aktivieren.
3. Klicken Sie auf **Speichern**.

Hinzufügen einer Authentifizierungsrichtlinie für die erstmalige Nutzung eines Browsers durch die Benutzer

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**. Klicken Sie unter „Verwaltete Geräte“ auf **BlackBerry Enterprise Identity**.
2. Klicken Sie im Bereich **Authentifizierungsrichtlinien** auf **Richtlinie hinzufügen**.
3. Geben Sie einen Namen und eine Beschreibung für die Authentifizierungsrichtlinie ein.
4. Wählen Sie in der Dropdown-Liste **Mindestauthentifizierungsebene** Ebene 1.

   Diese Ebene entspricht der Enterprise-Kennwort-Authentifikatorrangfolge, die Sie in der vorherigen Aufgabe festgelegt haben. Wenn Sie diese Richtlinie speichern, ohne ein Risikoszenario hinzuzufügen und es Benutzern zuzuweisen, müssen diese bei der Anmeldung bei einem Dienst nur ihr Enterprise-Kennwort eingeben. Wenn Sie eine zusätzliche Authentifizierung bei der erstmaligen Verwendung des Browsers verlangen möchten, führen Sie die folgenden Schritte durch, um ein Risikoszenario hinzuzufügen.
5. Klicken Sie in der Tabelle **Risikoszenarien** auf +.
6. Geben Sie einen Namenund eine Beschreibung für das Szenario ein.
7. Wählen Sie in der Dropdown-Liste **Mindestauthentifizierungsebene** Ebene 3. Diese Ebene entspricht der Enterprise-Kennwort- und BlackBerry 2FA-Authentifikatorrangfolge, die Sie in der vorherigen Aufgabe festgelegt haben.
8. Klicken Sie auf **Netzwerkerkennung**.
9. Wählen Sie in der Dropdown-Liste **Konfiguration** die Option **Browser erstmals erkannt**.

Wenn Sie diese Option konfigurieren und einer der Benutzer Ihres Unternehmens erstmals einen Browser verwendet und versucht, sich bei einem Dienst anzumelden, muss er sein Enterprise-Kennwort eingeben und auf eine BlackBerry 2FA-Aufforderung auf seinem Gerät reagieren.

10. Klicken Sie auf **Speichern**.
11. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Weisen Sie die Authentifizierungsrichtlinie Benutzern oder Gruppen zu.

Benutzerauthentifizierung mit PingFederate zulassen

BlackBerry Enterprise Identity kann die Authentifizierung an PingFederate weiterleiten, sodass vorhandene Ping Identity-Benutzer auf eine vertraute Benutzeroberfläche zugreifen können. BlackBerry Enterprise Identity- oder BlackBerry Intelligent Security-Richtlinien können zudem die Authentifizierung mit Ping Identity den Risiken und dem Kontext entsprechend angepasst werden, z. B. durch die PingID-Erweiterung oder die BlackBerry 2FA-Multifaktor-Authentifizierung.

Bevor die Kommunikation zwischen BlackBerry Enterprise Identity und PingFederate möglich ist, müssen Sie einen Ping Identity-Client auf dem PingFederate-Server Ihres Unternehmens und einen entsprechenden Identitätsanbieter in BlackBerry UEM erstellen.

Bevor Sie einen Ping Identity-Client erstellen, stellen Sie sicher, dass in der PingFederate-Authentifizierungsrichtlinie Ihres Unternehmens das Attribut OBJECTGUID auf Hex gesetzt ist. Weitere Informationen finden Sie in der Dokumentation von Ping Identity.

Hinweis: In Ihrer Umgebung muss die neueste Version von BlackBerry UEM 12.11 installiert sein.

Ping Identity-Client auf einem PingFederate-Server erstellen

Bevor sich Ihre BlackBerry Enterprise Identity-Benutzer mit PingFederate authentifizieren können, müssen Sie einen Ping Identity-Client auf dem PingFederate-Server Ihres Unternehmens einrichten.

1. Melden Sie sich bei der PingFederate-Verwaltungskonsole an.
2. Klicken Sie auf **OAuth-Server**.
3. Klicken Sie in der Spalte „Clients“ auf **Neu erstellen**.
4. Geben Sie im Feld **Client-ID** eine eindeutige ID für den Client ein. Beachten Sie, dass diese ID verwendet wird, wenn Sie den Identitätsanbieter in BlackBerry UEM einrichten.
5. Geben Sie einen Namen und eine Beschreibung für den Client ein.
6. Klicken Sie im Abschnitt „Client-Authentifizierung“ auf **Privater Schlüssel: JWT**.
7. Wählen Sie die Option **Signierte Anfragen anfordern** aus.
8. Um einen JSON-Webschlüsselsatz zu erstellen, gehen Sie zu https://mkjwk.org/.
9. Klicken Sie auf die Registerkarte **Elliptische Kurve**.
10. Wählen Sie in der Dropdown-Liste **Kurve** die Option **P-256** aus.
11. Wählen Sie in der Dropdown-Liste **Algorithmus** die Option **ES256** aus.
12. Klicken Sie auf **Neuer Schlüssel**.
13. Kopieren Sie den Schlüssel aus dem Feld **Schlüsselpaar-Satz**. Beachten Sie, dass Sie denselben Schlüssel in Schritt Identitätsanbieter in BlackBerry UEM konfigurieren verwenden.
14. Fügen Sie den Schlüssel in das Feld **JWKS** auf der PingFederate-Website ein.
15. Fügen Sie im Feld **URI umleiten** den URI des PingFederate-Servers Ihres Unternehmens hinzu, und klicken Sie auf **Hinzufügen**.

16. Wählen Sie im Abschnitt **Erteilte Berechtigungen** die Option **Autorisierungscode** aus.
17. Wählen Sie in der Dropdown-Liste **Signaturalgorithmus des ID-Tokens** eine der **ECDSA**-Optionen aus. Beachten Sie, dass Sie dieselbe Option in Schritt Identitätsanbieter in BlackBerry UEM konfigurieren verwenden.
18. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Identitätsanbieter in BlackBerry UEM konfigurieren

Identitätsanbieter in BlackBerry UEM konfigurieren

Nachdem Sie einen Ping Identity-Client erstellt haben, müssen Sie einen entsprechenden Identitätsanbieter in der BlackBerry UEM-Verwaltungskonsole erstellen.

Bevor Sie beginnen: Ping Identity-Client auf einem PingFederate-Server erstellen

1. Klicken Sie in der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > BlackBerry Enterprise Identity > Identitätsanbieter**.
2. Klicken Sie auf **+**, und wählen Sie **PingFederate** aus.
3. Geben Sie im Feld **Name** einen Namen für den Identitätsanbieter ein.
4. Geben Sie im Feld **URL für das OIDC-Erkennungsdokument** den Speicherort des PingFederate-Servers Ihres Unternehmens ein.
5. Geben Sie im Feld **Client-ID** die gleiche ID ein, die Sie im Thema Ping Identity-Client auf einem PingFederate-Server erstellen verwendet haben.
6. Geben Sie in das Feld **Privater Schlüssel: JWKS** denselben Schlüssel ein, den Sie im Thema Ping Identity-Client auf einem PingFederate-Server erstellen verwendet haben.
7. Wählen Sie in der Dropdown-Liste **Signaturalgorithmus des ID-Tokens** die gleiche Option aus, die Sie im Thema Ping Identity-Client auf einem PingFederate-Server erstellen ausgewählt haben.
8. Wählen Sie in der Liste **Verfügbare Dienste** die Dienste aus, die Sie dem Ping Identity-Client zuweisen möchten, und klicken Sie auf den Pfeil nach rechts, um den Dienst in die Liste **Ausgewählte Dienste** zu verschieben. Beachten Sie, dass Sie jedem Dienst nur einen Ping Identity-Client zuweisen können.
9. Klicken Sie auf **Speichern**.

Erstellen einer BlackBerry Enterprise Identity-Richtlinie für Benutzer von PingFederate

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Konsole auf **Richtlinien und Profile > BlackBerry Enterprise Identity > Richtlinie hinzufügen**.
2. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
3. Wählen Sie auf dem Bildschirm **Einstellungen > BlackBerry Enterprise Identity > Einstellungen** in der Dropdown-Liste **Minimale Authentifikatorebene** die Nummer aus, die einer der Authentifizierungsebenen für Ping Identity entspricht. Sie können eine Ebene auswählen, die den folgenden Optionen entspricht: Ping-Kennwort, Ping-Kennwort + BlackBerry 2FA oder Ping-Kennwort + PingID.
4. Optional können Sie ein Risikoszenario hinzufügen, das zusätzliche Sicherheit bietet, wenn bestimmte Bedingungen vorliegen, z. B. wenn sich ein Benutzer nicht in einem internen Netzwerk befindet. Klicken Sie in der Tabelle **Risikoszenarien** auf **+**.
5. Geben Sie einen Namenund eine Beschreibung für das Risikoszenario ein.
6. Wählen Sie auf dem Bildschirm „Einstellungen > BlackBerry Enterprise Identity > Einstellungen“ eine der Authentifizierungsebene für Ping entsprechende Mindestauthentifizierungsebene aus. Sie können festlegen, dass Ihre Benutzer nur ihr Kennwort eingeben, auf eine BlackBerry 2FA-Eingabeaufforderung antworten oder ihre PingID eingeben können, wenn bei der Anmeldung des Benutzers bei dem Dienst einer der Risikofaktoren vorhanden ist. Die folgenden Risikofaktoren sind verfügbar:

- **Netzwerkerkennung**: Wenn Sie herausfinden möchten, ob die App oder der Browser eines Benutzers mit demselben Netzwerk wie der BlackBerry UEM-Server verbunden ist, wählen Sie die Option „Netzwerkerkennung“, und wählen Sie in der Dropdown-Liste „Konfiguration“ die gewünschte Option aus.
- **Browsererkennung**: Wenn Sie eine Vertrauensreferenz zwischen dem Browser und Enterprise Identity beim ersten Öffnen eines Browsers durch den Benutzer herstellen möchten, wählen Sie die Option „Browser-Erkennung“, und wählen Sie in der Dropdown-Liste „Konfiguration“ die gewünschte Option aus.
- **BlackBerry Persona**: Wenn Sie Risikoebenen und Geozonen von BlackBerry Persona Mobile als Risikofaktoren verwenden möchten, wählen Sie die Option BlackBerry Persona aus.

7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Weisen Sie die Richtlinie den PingFederate-Benutzern Ihres Unternehmens zu. Wenn Ihre Benutzer in einer Gruppe konfiguriert sind, können Sie das Thema Zuweisen einer Enterprise Identity-Richtlinie zu einer Benutzergruppe befolgen, um die Richtlinie problemlos allen Benutzern gleichzeitig zuzuweisen.

Benutzerauthentifizierung mit Okta zulassen

BlackBerry Enterprise Identity kann die Authentifizierung an Okta umleiten, sodass vorhandene Okta-Benutzer auf eine vertraute Benutzeroberfläche zugreifen können. Mit BlackBerry Enterprise Identity- oder BlackBerry Persona-Richtlinien können zudem die Authentifizierung mit Okta den Risiken und dem Kontext entsprechend angepasst werden, z. B. durch die BlackBerry 2FA-Multifaktor-Authentifizierung.

Bevor die Kommunikation zwischen BlackBerry Enterprise Identity und PingFederate möglich ist, müssen Sie einen Ping Identity-Client auf dem PingFederate-Server Ihres Unternehmens und einen entsprechenden Identitätsanbieter in BlackBerry UEM erstellen.

Bevor Sie einen Ping Identity-Client erstellen, stellen Sie sicher, dass in der PingFederate-Authentifizierungsrichtlinie Ihres Unternehmens das Attribut OBJECTGUID auf Hex gesetzt ist. Weitere Informationen finden Sie in der Dokumentation von Ping Identity.

Hinweis: In Ihrer Umgebung muss die neueste Version von BlackBerry UEM 12.11 installiert sein.

Erstellen einer Okta-App

Bevor Sie beginnen:

Ihre Okta-Instanz muss über eine Verbindung zu Microsoft Active Directory verfügen, und Ihre Benutzer müssen in Okta importiert werden. Anweisungen finden Sie unter https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-main.htm

1. Melden Sie sich bei der Okta-Verwaltungskonsole an.
2. Erstellen Sie ein Sicherheitstoken.
   a) Klicken Sie auf **Sicherheit** > **API** > **Token**.
   b) Klicken Sie auf **Token erstellen**.
   c) Kopieren Sie das Token.
3. Generieren Sie die JWKS-Schlüssel.
   a) Rufen Sie die Website https://mkjwk.org auf.
   b) Klicken Sie auf die Registerkarte **EC**.
   c) Wählen Sie in der Dropdown-Liste **Kurve** die Option **P-521** aus.
   d) Wählen Sie in der Dropdown-Liste **Algorithmus** die Option **ES521: ECDSA mit P-521 und SHA-512** aus.
   e) Wählen Sie in der Dropdown-Liste **Schlüssel-ID** die Option **SHA-256** aus.

f) Kopieren Sie das öffentliche und private Schlüsselpaar, den Schlüsselpaarsatz und den öffentlichen Schlüssel.

Hinweis: In den öffentlichen und privaten Schlüsselpaarsätzen müssen Sie das Attribut **„d“:** entfernen, da es sich um einen privaten Schlüssel handelt.

4. Verwenden Sie in einer Eingabeaufforderung eine CURL/Postman-Anforderung, um eine OIDC-App mit Okta zu registrieren und die folgenden Felder in JSON zu aktualisieren. Das Erstellen dieser Art von App wird derzeit in der Okta-Konsole nicht unterstützt.

- Stellen Sie sicher, dass der SSWS-Autorisierungswert das Token ist, das Sie in Schritt 2 erstellt haben.
- Ersetzen Sie die JWKS-Schlüssel mit den Schlüsseln aus Schritt 3.
- Stellen Sie sicher, dass das Attribut „d;“ entfernt wurde.

Ihre Eingabe sollte der folgenden ähneln.

```
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"
                    }
                ]
            }
        }
    }
}'
```

Informationen zur JSON-Spezifikation finden Sie unter https://developer.okta.com/docs/reference/api-overview/

5. Zeigen Sie Ihre App in der Okta-Konsole an, und kopieren Sie die **Client-ID**.
6. Weisen Sie die App Benutzern zu. Anweisungen finden Sie unter https://help.okta.com/en/prod/Content/Topics/Provisioning/lcm/lcm-user-app-assign.htm.
7. Um Okta ID-Ansprüche einzurichten, gehen Sie zu **Sicherheit** > **API** > **Autorisierungsserver**, und wählen Sie Ihren Autorisierungsserver aus.
8. Klicken Sie auf der Registerkarte **Ansprüche** auf **Ansprüche hinzufügen**, und fügen Sie einen Anspruch mit den folgenden Werten hinzu:
   a) **Name**: object_guid
   b) **In Tokentyp einschließen**: Immer ID-Token
   c) **Werttyp**: Ausdruck
   d) **Wert**: findDirectoryUser().externalId
9. Klicken Sie auf **Erstellen**.

Konfigurieren von Okta als Identitätsanbieter in BlackBerry UEM

Nachdem Sie einen Okta-Client erstellt haben, müssen Sie einen entsprechenden Identitätsanbieter in der BlackBerry UEM-Verwaltungskonsole erstellen.

Bevor Sie beginnen: Erstellen einer Okta-App

1. Klicken Sie in der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > BlackBerry Enterprise Identity > Identitätsanbieter**.
2. Klicken Sie auf **+**, und wählen Sie **Okta** aus.
3. Geben Sie im Feld **Name** einen Namen für den Identitätsanbieter ein.
4. Geben Sie im Feld **URL für das OIDC-Erkennungsdokument** den Speicherort des Okta-Servers Ihres Unternehmens ein. Beispiel: `https://<oktaDomina>.okta.com/.well-known/oauth-authorization`
5. Geben Sie im Feld **Client-ID** die Client-ID ein, die Sie in Schritt Erstellen einer Okta-App erstellt haben.
6. Geben Sie im Feld **Privater Schlüssel JWKS** den privaten Schlüssel ein, den Sie in Schritt Erstellen einer Okta-App erstellt haben.

   Ihre Eingabe sollte der folgenden ähneln.

```
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. Wählen Sie in der Liste **Verfügbare Dienste** die Dienste aus, die Sie dem Okta-Client zuweisen möchten, und klicken Sie auf den Pfeil nach rechts, um den Dienst in die Liste **Ausgewählte Dienste** zu verschieben. Beachten Sie, dass Sie jedem Dienst nur einen Okta-Client zuweisen können.
8. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Erstellen einer Enterprise Identity-Authentifizierungsrichtlinie und weisen Sie es Benutzern oder Gruppen zu. Fügen Sie in der Richtlinie Ihren Service unter „Dienstausnahmen verwalten“ hinzu, und legen Sie die minimale Authentifizierungsebene auf Ebene 4 fest.

Verwalten von App-Gruppen

Sie können App-Gruppen verwenden, um eine App-Sammlung in BlackBerry UEM zu erstellen und sie Benutzern, Benutzergruppen oder Gerätegruppen zuzuweisen. Die Gruppierung von Apps steigert die Effizienz und Konsistenz bei der Verwaltung von Apps. Beispielsweise können Sie App-Gruppen nutzen, um die gleiche App für mehrere Gerätetypen zu gruppieren oder Apps für Benutzer mit der gleichen Rolle innerhalb Ihrer Organisation zu gruppieren. Mit BlackBerry Enterprise Identity kann eine App-Gruppe für einen bestimmten Dienst zusätzlich zu den mobilen App-Quelldateien auch die Single Sign-On-Berechtigung umfassen. Somit haben Benutzer alles, was sie benötigen, um auf den Dienst mit einer einzigen Aktion zuzugreifen.

Sie können App-Gruppen über die BlackBerry UEM-Verwaltungskonsole verwalten. Weitere Informationen finden Sie in der BlackBerry UEM Dokumentation für Administratoren unter Verwalten von App-Gruppen.

Zuweisen von Berechtigungen an Benutzer oder Gruppen

Bevor Sie beginnen: Sie müssen zuerst Benutzer und Dienste in BlackBerry UEM hinzufügen, bevor Sie Benutzern Berechtigungen für bestimmte Dienste zuweisen können. Informationen zum Hinzufügen von Diensten finden Sie im Handbuch unter Integrieren von SaaS-Diensten. Sobald die Enterprise Identity-Dienste mit BlackBerry UEM synchronisiert wurden, sind diese in der Verwaltungskonsole als Apps verfügbar. Sie können einem Benutzer eine App zuweisen, sodass dieser den Dienst nutzen kann.

1. Wählen Sie in der BlackBerry UEM-Verwaltungskonsole den Benutzer oder die Benutzergruppe aus, der Sie Berechtigungen zuweisen möchten. Führen Sie eine der folgenden Aktionen aus:
   - Um Benutzern Berechtigungen zuzuweisen, klicken Sie in der Menüleiste auf **Benutzer**, und wählen Sie deren Namen aus.
   - Um Benutzergruppen Berechtigungen zuzuweisen, klicken Sie in der Menüleiste auf **Gruppen**, und wählen Sie die Gruppen aus. Klicken Sie auf die Registerkarte **Einstellungen**.
2. Wählen Sie die App oder App-Gruppe aus, die Sie zuweisen möchten.
3. Aktivieren Sie das Kontrollkästchen neben dem zuzuweisenden Dienst.
4. Klicken Sie auf **Zuweisen**.
5. Wenn Sie aufgefordert werden, Lizenzen zuzuweisen, klicken Sie auf **Ja**.

Ändern der Enterprise Identity-Einstellungen

Einige BlackBerry Enterprise Identity-Einstellungen können über die BlackBerry UEM-Verwaltungskonsole angepasst werden. Sie können den Anzeigenamen von Anmeldeinformationen auf der Enterprise Identity-Anmeldeseite ändern. Außerdem können Sie die Rangfolge von Authentifikatoren anpassen. Der Authentifizierungsprozess für Dienste beginnt mit dem ranghöchsten Authentifikator und wird die Liste abwärts fortgesetzt.

1. Klicken Sie in der Menüleiste auf **Einstellungen** > **BlackBerry Enterprise Identity**.
2. Sie können den benutzerfreundlichen Namen für Ihre BlackBerry UEM-Anmeldedaten im Textfeld „Name“ eingeben oder ändern.
3. Um den Rang von Authentifikatoren zu ändern, klicken Sie auf die nach oben oder unten zeigenden Pfeile in der Spalte **Rangfolge**. Mobiles ZSO wird von keinem der Dienste unterstützt. Wenn dieser Authentifikator den ersten Platz auf der Liste belegt, sind einige Dienste nicht verfügbar.
4. Klicken Sie auf **Speichern**.

Anpassen der Benutzeranmeldeseite Ihres Unternehmens

Sie können die BlackBerry Enterprise Identity Benutzeranmeldeseite Ihres Unternehmens anpassen. Sie können zum Beispiel das Logo Ihres Unternehmens hinzufügen.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**.
2. Klicken Sie auf **App hinzufügen**.
3. Klicken Sie auf **Enterprise Identity**. In einer Meldung wird die Frage angezeigt, ob Sie Enterprise Identity Services synchronisieren möchten.
4. Klicken Sie auf **Enterprise Identity-Konsole öffnen**. Die Administratorkonsole wird in einer neuen Browserregisterkarte geöffnet. Falls die Konsole nicht geöffnet wird, stellen Sie sicher, dass Sie die Pop-ups in Ihrem Browser aktiviert haben.
5. Klicken Sie auf **Enterprise**.
6. Geben Sie im Feld **Anmeldesicherheitstext** alle zusätzlichen Informationen ein, die Ihre Benutzer wissen sollten. Dieser Text wird auf der Anmeldeseite unter dem Feld „Kennwort“ angezeigt.
7. Geben Sie im Feld **Anmeldetitel** den Text ein, der oben auf der BlackBerry Enterprise Identity-Anmeldeseite Ihres Unternehmens angezeigt werden soll. Sie können die Dropdown-Liste **Token einfügen** verwenden, um den Anmeldetiteltext zu formatieren.
8. Geben Sie im Feld **Beschreibung des Benutzernamens** den Text ein, der über dem Textfeld „Benutzername“ auf der BlackBerry Enterprise Identity-Anmeldeseite Ihres Unternehmens angezeigt werden soll. Mithilfe der Dropdown-Liste **Token einfügen** können Sie den Text für die Beschreibung des Benutzernamens formatieren.
9. Geben Sie im Feld **Beschreibung des Kennworts** den Text ein, der über dem Textfeld „Kennwort“ auf der BlackBerry Enterprise Identity-Anmeldeseite Ihres Unternehmens angezeigt wird. Mithilfe der Dropdown-Liste **Token einfügen** können Sie den Text für die Beschreibung des Kennworts formatieren.
10. Klicken Sie im Feld **Logo** auf **Datei auswählen**, um zur BlackBerry Enterprise Identity-Anmeldeseite Ihres Unternehmens zu navigieren und ein Logo hinzuzufügen.
11. Wählen Sie Optionen für die Felder **Logo-Stil**, **Textfarbe** und **Hintergrund** aus.
12. Klicken Sie auf **Speichern**.

SAML-ECP-Unterstützung für Microsoft Office 365

Einige mobile E-Mail-Clients, darunter einige Versionen von BlackBerry Hub und BlackBerry Work, bieten keine Unterstützung für die Microsoft ADAL-Schnittstelle bei Verwendung mit Microsoft Office 365, sodass die normale Anmeldungs-UI von BlackBerry Enterprise Identity nicht angezeigt werden kann. Um diese Funktion für mobile E-Mail-Clients zu aktivieren, können Sie die ECP-Unterstützung (Profil „Enhanced Client or Proxy“) von Enterprise Identity für Office 365 aktivieren, die die Authentifizierung mit Text-basierten Anmeldeinformationen, wie Benutzername und Kennwort, ermöglicht. Diese Anmeldedaten werden dann von der eigenen Benutzeroberfläche des E-Mail-Clients abgerufen. Beachten Sie, dass bei Verwendung von ECP für Office 365 die Enterprise Identity-Authentifizierungsrichtlinien nicht auf ECP-basierte Anmeldungen angewendet werden.

Aktivieren der ECP-Unterstützung für Office 365

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**.
2. Klicken Sie auf **App hinzufügen**.
3. Klicken Sie auf **Enterprise Identity**.
4. Klicken Sie auf **Enterprise Identity-Konsole öffnen**. Die Administratorkonsole wird in einer neuen Browserregisterkarte geöffnet. Falls die Konsole nicht geöffnet wird, stellen Sie sicher, dass Sie die Pop-ups in Ihrem Browser aktiviert haben.
5. Ändern Sie auf der Seite **Unternehmen** die Option **ECP-Unterstützung für Microsoft Office 365** zu **Ein**.
6. Klicken Sie auf **Speichern**.

Verhindern, dass Benutzerkonten gesperrt werden

Sie können BlackBerry Enterprise Identity so konfigurieren, dass Benutzerkonten von beispielsweise Active Directory-Benutzern nicht aufgrund von zu vielen fehlgeschlagenen Anmeldeversuchen bei BlackBerry Enterprise Identity gesperrt werden.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**.
2. Klicken Sie auf **App hinzufügen**.
3. Klicken Sie auf **Enterprise Identity**. In einer Meldung wird die Abfrage angezeigt, ob Sie die Enterprise Identity-Services synchronisieren möchten.
4. Klicken Sie auf **Enterprise Identity-Konsole öffnen**. Die Administratorkonsole wird in einer neuen Browserregisterkarte geöffnet. Falls die Konsole nicht geöffnet wird, stellen Sie sicher, dass Sie die Pop-ups in Ihrem Browser aktiviert haben.
5. Klicken Sie auf **Enterprise**.
6. Aktivieren Sie im Abschnitt **Kontosperreinstellungen** die Option **Kontosperrung aktivieren**.
7. Legen Sie die folgenden Optionen fest:
   - **Schwellenwert für Anmeldeversuche**: Legt die Anzahl der fehlgeschlagenen Versuche fest, bevor das Konto vorübergehend gesperrt wird.
   - **Anmeldedauer (Minuten**): Legt die Anzahl der Minuten fest, für die ein Konto gesperrt wird. Nach dieser Zeit sollte das Konto für den nächsten Anmeldeversuch entsperrt sein.
   - **Reset-Dauer (Minuten)**: Legt die Anzahl der Minuten fest, die nach einem fehlgeschlagenen Anmeldeversuch verstreichen müssen, bevor der Zähler für fehlgeschlagene Anmeldeversuche auf 0 zurückgesetzt wird.
8. Klicken Sie auf **Speichern**.

Auswahl von Mandant und Domäne

Die meisten Benutzer melden sich bei Enterprise Identity mit einem Benutzernamen und Kennwort an. Darüber hinaus geben sie an, ob der Browser vertrauenswürdig ist. Falls ein Benutzername in mehreren Mandanten oder Domänen vorhanden ist, muss der Benutzer bei der erstmaligen Anmeldung den Mandanten aus einer Dropdown-Liste auswählen oder die Domäne eingeben. Die getroffene Auswahl wird für nachfolgende Anmeldungen gespeichert.

Verwalten von BlackBerry UEM-Mandanten in der BlackBerry Enterprise Identity-Konsole

Um die BlackBerry UEM-Mandanten Ihres Unternehmens zu verwalten, können Sie die Seite für UEM-Mandanten in der Enterprise Identity-Konsole verwenden. Sie können die Eigenschaften der Mandanten bearbeiten oder die Mandanten deaktivieren. Beachten Sie, dass beim Deaktivieren eines Mandanten die Authentifizierung von Benutzern Ihres Unternehmens mit den Enterprise Identity-Diensten, die Sie in BlackBerry UEM aktiviert haben, nicht möglich ist.

Sie können die folgenden Eigenschaften von BlackBerry UEM-Mandanten bearbeiten.

Objekt	Beschreibung
Anzeigename	Ändern Sie den Anzeigenamen des Mandanten. Dieser Name wird in der UEM-Mandantenauswahl auf dem Anmeldebildschirm angezeigt, wenn ein Benutzer in mehr als einem UEM-Mandanten vorhanden ist.
Authentifikatortypen – AD	Schalten Sie die verknüpfte Microsoft Active Directory-Instanz ein oder aus, und ändern Sie den Anzeigenamen der Active Directory-Instanz.
Authentifikatortypen – LDAP	Schalten Sie das verknüpfte LDAP-Verzeichnis ein oder aus, und ändern Sie den Anzeigenamen des LDAP-Verzeichnisses.
Erkennung geschäftlicher Netzwerke	Schalten Sie die Netzwerkerkennung ein oder aus. Mit diesem Risikofaktor wird geprüft, ob die App oder der Browser von Benutzern mit demselben Netzwerk wie der BlackBerry UEM-Server verbunden ist.

Verwalten von Administratoren und Benutzern

Sie können Administratoren und Benutzer hinzufügen oder entfernen oder deren Berechtigungen in der BlackBerry UEM-Verwaltungskonsole ändern. Weitere Informationen zum Verwalten von Administratoren und Benutzern finden Sie in der BlackBerry UEM-Dokumentation für Administratoren.

Wenn Sie BlackBerry UEM aus irgendeinem Grund neu bereitstellen müssen, müssen Sie zunächst alle Benutzer mit Berechtigungen für Enterprise Identity aus BlackBerry UEM entfernen. Wenn Benutzer vor einer Neubereitstellung von BlackBerry UEM nicht entfernt werden, sind ihnen möglicherweise weiterhin Dienste zugewiesen, auf die sie aber nicht zugreifen können.

Erstellen eines benutzerdefinierten Enterprise Identity Administrators

Mit Hilfe von Administratorrollen können Sie bestimmte BlackBerry Enterprise Identity administrative Aufgaben an Benutzer delegieren. Die Rolle des Sicherheitsadministrators in BlackBerry UEM verfügt über volle Berechtigungen für die Verwaltungskonsole – einschließlich der Erstellung und Verwaltung von Rollen und Administratoren. Mindestens ein Administrator muss ein Sicherheitsadministrator sein. BlackBerry UEM enthält neben der Rolle des Sicherheitsadministrators vorkonfigurierte Rollen. Sie können alle Rollen – mit Ausnahme der Rolle des Sicherheitsadministrators – bearbeiten oder löschen. Sie können auch benutzerdefinierte Rollen erstellen.

Hinweis: Alle neuen benutzerdefinierten BlackBerry Enterprise Identity Administratoren, die Sie erstellen, können keine BlackBerry Enterprise Identity Berechtigungen, Apps oder App-Gruppen an Benutzer oder Benutzergruppen zuweisen. Weitere Informationen finden Sie unter Zuweisen von Berechtigungen an Benutzer oder Gruppen und Verwalten von App-Gruppen.

Bevor Sie beginnen:

- Nur Sicherheitsadministratoren können eine benutzerdefinierte Rolle erstellen.

1. Klicken Sie im linken Menü auf **Einstellungen > Administratoren > Rollen**.
2. Klicken Sie auf das .
3. Geben Sie einen Namen und eine Beschreibung für die Rolle ein.
4. Wählen Sie die Enterprise Identity-Richtlinienoptionen im Abschnitt **Richtlinien und Profile** aus. Die Auswahlmöglichkeiten sind: **Enterprise-Identity-Authentifizierungsrichtlinie anzeigen, Authentifizierungsrichtlinie erstellen oder bearbeiten, Authentifizierungsrichtlinie löschen** und **Authentifizierungsrichtlinie an Benutzer und Gruppen zuweisen**.
5. Wählen Sie die Enterprise Identity-Optionen im Abschnitt **Einstellungen** aus. Die Auswahlmöglichkeiten sind: **Enterprise-Identity-Unternehmenseinstellungen anzeigen, Enterprise-Identity-Unternehmenseinstellungen bearbeiten, Enterprise Identity-Dienste anzeigen** und **Enterprise Identity-Dienste bearbeiten**.
6. Klicken Sie auf **Speichern**.
7. Fügen Sie die Rolle einem Benutzerkonto oder einer Benutzergruppe hinzu.

Wenn Sie fertig sind:

Weitere Informationen über Rollen finden Sie in der BlackBerry UEM-Dokumentation für Administratoren.

Rechtliche Hinweise

DARGELEGT AUSGESCHLOSSEN WERDEN KÖNNEN, HIERMIT AUF 90 TAGE AB DATUM DES ERWERBS DER DOKUMENTATION ODER DES ARTIKELS, AUF DEN SICH DIE FORDERUNG BEZIEHT, BESCHRÄNKT.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS HAFTET BLACKBERRY UNTER KEINEN UMSTÄNDEN FÜR SCHÄDEN JEGLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEGLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE, VERSCHÄRFTEN SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE, STRAFE EINSCHLIESSENDE SCHÄDEN, FOLGESCHÄDEN ODER SCHÄDEN, FÜR DIE ANSPRUCH AUF KOMPENSATORISCHEN SCHADENERSATZ BESTEHT, SCHÄDEN WEGEN ENTGANGENEN GEWINNEN ODER EINKOMMEN, NICHTREALISIERUNG ERWARTETER EINSPARUNGEN, BETRIEBSUNTERBRECHUNGEN, VERLUST GESCHÄFTLICHER DATEN, ENTGANGENE GESCHÄFTSCHANCEN ODER BESCHÄDIGUNG BZW. VERLUST VON DATEN, DAS UNVERMÖGEN, DATEN ZU ÜBERTRAGEN ODER ZU EMPFANGEN, PROBLEME IM ZUSAMMENHANG MIT ANWENDUNGEN, DIE IN VERBINDUNG MIT BLACKBERRY-PRODUKTEN UND -DIENSTEN VERWENDET WERDEN, KOSTEN VON AUSFALLZEITEN, NICHTVERWENDBARKEIT VON BLACKBERRY-PRODUKTEN UND -DIENSTEN ODER TEILEN DAVON BZW. VON MOBILFUNKDIENSTEN, KOSTEN VON ERSATZGÜTERN, DECKUNG, EINRICHTUNGEN ODER DIENSTEN, KAPITAL- ODER ANDERE VERMÖGENSSCHÄDEN, UNABHÄNGIG DAVON, OB SCHÄDEN DIESER ART ABZUSEHEN ODER NICHT ABZUSEHEN WAREN, UND AUCH DANN, WENN BLACKBERRY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS ÜBERNIMMT BLACKBERRY KEINERLEI VERANTWORTUNG, VERPFLICHTUNG ODER HAFTUNG, SEI SIE VERTRAGLICHER, DELIKTRECHTLICHER ODER ANDERWEITIGER NATUR, EINSCHLIESSLICH DER HAFTUNG FÜR FAHRLÄSSIGKEIT UND DER DELIKTSHAFTUNG.

DIE IN DIESEM DOKUMENT GENANNTEN EINSCHRÄNKUNGEN, AUSSCHLÜSSE UND HAFTUNGSAUSSCHLÜSSE GELTEN (A) UNGEACHTET DER VON IHNEN ANGEFÜHRTEN KLAGEGRÜNDE, FORDERUNGEN ODER KLAGEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF VERTRAGSBRUCH, FAHRLÄSSIGKEIT, ZIVILRECHTLICHER DELIKTE, DELIKTSHAFTUNG ODER SONSTIGE RECHTSTHEORIE UND SIND AUCH NACH EINEM WESENTLICHEN VERSTOSS BZW. EINEM FEHLENDEN GRUNDLEGENDEN ZWECK DIESER VEREINBARUNG ODER EINES DARIN ENTHALTENEN RECHTSBEHELFS WIRKSAM; UND GELTEN (B) FÜR BLACKBERRY UND DIE ZUGEHÖRIGEN UNTERNEHMEN, RECHTSNACHFOLGER, BEVOLLMÄCHTIGTEN, VERTRETER, LIEFERANTEN (EINSCHLIESSLICH MOBILFUNKANBIETERN), AUTORISIERTE BLACKBERRY-DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH MOBILFUNKANBIETERN) UND DIE JEWEILIGEN FÜHRUNGSKRÄFTE, ANGESTELLTEN UND UNABHÄNGIGEN AUFTRAGNEHMER.

ZUSÄTZLICH ZU DEN OBEN GENANNTEN EINSCHRÄNKUNGEN UND AUSSCHLÜSSEN HAFTEN DIE FÜHRUNGSKRÄFTE, ANGESTELLTEN, VERTRETER, DISTRIBUTOREN, LIEFERANTEN, UNABHÄNGIGEN AUFTRAGNEHMER VON BLACKBERRY ODER BLACKBERRY ANGEHÖRENDEN UNTERNEHMEN IN KEINER WEISE IM ZUSAMMENHANG MIT DER DOKUMENTATION.

Bevor Sie Drittprodukte bzw. -dienste abonnieren, installieren oder verwenden, müssen Sie sicherstellen, dass Ihr Mobilfunkanbieter sich mit der Unterstützung aller zugehörigen Funktionen einverstanden erklärt hat. Einige Mobilfunkanbieter bieten möglicherweise keine Internet-Browsing-Funktion in Zusammenhang mit einem Abonnement für den BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem Dienstanbieter bezüglich Verfügbarkeit, Roaming-Vereinbarungen, Mobilfunktarifen und Funktionen. Für die Installation oder Verwendung von Drittprodukten und -diensten mit den Produkten und Diensten von BlackBerry sind u. U. Patent-, Marken-, Urheberrechts- oder sonstige Lizenzen erforderlich, damit die Rechte Dritter nicht verletzt werden. Es liegt in Ihrer Verantwortung, zu entscheiden, ob Sie Drittprodukte und -dienste verwenden möchten, und festzustellen, ob hierfür Lizenzen erforderlich sind. Für den Erwerb etwaiger Lizenzen sind Sie verantwortlich. Installieren oder verwenden Sie Drittprodukte und -dienste erst nach dem Erwerb aller erforderlichen Lizenzen. Alle Drittprodukte und -dienste, die Sie mit Produkten und Diensten von BlackBerry erhalten, werden lediglich zu Ihrem Vorteil, OHNE MÄNGELGEWÄHR und ohne ausdrückliche oder stillschweigende Bedingung, Billigung, Garantie, Zusicherung oder Gewährleistung jedweder Art von BlackBerry bereitgestellt. BlackBerry übernimmt in diesem Zusammenhang keinerlei Haftung. Die Verwendung von Drittprodukten und -diensten unterliegt Ihrer Zustimmung zu den

Bedingungen separater Lizenzen und anderer geltender Vereinbarungen mit Dritten, sofern sie nicht ausdrücklich von einer Lizenz oder anderen Vereinbarung mit BlackBerry abgedeckt wird.

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE PASSAGE IN DIESEM DOKUMENT IST DAZU VORGESEHEN, BELIEBIGE SCHRIFTLICHE VEREINBARUNGEN ODER GARANTIEN, DIE VON BLACKBERRY FÜR TEILE VON BELIEBIGEN BLACKBERRY-PRODUKTEN ODER -DIENSTLEISTUNGEN AN ANDERER STELLE ALS IN DIESER DOKUMENTATION ANGEGEBEN WURDEN, ZU ERSETZEN.

BlackBerry Enterprise Software enthält bestimmte Softwarekomponenten von Drittanbietern. Die mit der Software verbundenen Lizenz- und Copyright-Informationen finden Sie unter: http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

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

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

Veröffentlicht in Kanada