BlackBerry Enterprise Identity

Integrationshandbuch

Inhalt

Was ist BlackBerry Enterprise Identity ?

BlackBerry Enterprise Identity bietet 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 wird mit BlackBerry UEM, BlackBerry UEM Cloud oder BES12 gebündelt. Administratoren nutzen die BlackBerry UEM-, BlackBerry UEM Cloud- oder BES12-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 10 und 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.

Einrichten von BlackBerry Enterprise Identity und des SaaS-Clients

Um sicherzustellen, dass BlackBerry Enterprise Identity und der SaaS-Client Ihres Unternehmens zusammenarbeiten können, müssen Sie folgende Aufgaben durchführen:

- Erstellen eines Zertifikats und Schlüsselpaars
- Konfigurieren einer neuen SAML-Verbindung im SaaS-Client
- Erstellen eines SaaS-Dienstes in der BlackBerry UEM-Konsole oder Erstellen eines SaaS-Dienstes in der BlackBerry Enterprise Identity-Konsole

Erstellen eines Zertifikats und Schlüsselpaars

Das Zertifikat und das Schlüsselpaar sind erforderlich, damit der jeweilige Dienst funktioniert. Sie laufen in regelmäßigen Abständen ab und müssen dann neu erstellt werden. Ihr Unternehmen setzt möglicherweise ein eigenes Verfahren zum Erstellen von Zertifikaten und Schlüsseln ein. Es besteht beispielsweise eine vertragliche Vereinbarung mit einer der Firmen, die Zertifikate verkaufen. Diese Aufgabe beschreibt, wie Sie ein selbstsigniertes Zertifikat erstellen, das möglicherweise nicht für alle Unternehmen geeignet ist und in der Regel nicht die höchste Sicherheit bietet. Die Verwaltung der Schlüssel ist wichtig, um die Sicherheit zu gewährleisten.

1. Laden Sie OpenSSL herunter. Verwenden Sie unter Windows den Win32 OpenSSL Light Installer.
2. Geben Sie Folgendes in das Eingabeaufforderungsfenster ein:
   - `cd \OpenSSL-Win32\bin.`
   - `openssl req -newkey rsa:2048 -nodes -keyout private.key -x509 -days 730 -out certificate.pem`

   Wenn Sie von OpenSSL dazu aufgefordert werden, verwenden Sie die folgenden Werte:

   Country Name (aus 2 Buchstaben bestehender Code) [AU]:CA State or Province Name (vollständiger Name) [Ontario]: Locality Name (z. B. Stadt) [Waterloo]: Organization Name (z. B. Unternehmen) [Internet Widgits Pty Ltd]: Organizational Unit Name [Marketing]:BlackBerry Identity Common Name (z. B., Server-FQDN oder IHR Name) [example.fqdn]:ServiceName Email Address [myoffice365@email.com]:
3. Speichern Sie die Schlüsseldatei, und legen Sie sie an einem sicheren Ort ab (z. B. einem Schlüsselspeicher). Der Schlüssel sollte verschlüsselt und durch Kennwort geschützt sein. Das Zertifikat wird in die Dienstmetadaten aufgenommen und kann gemeinsam genutzt werden.

Konfigurieren einer neuen SAML-Verbindung im SaaS-Client

1. Melden Sie sich bei der SaaS-Client-Anwendung als Administrator an.
2. Suchen Sie nach der SAML-Einrichtungsseite. Einige Services bieten eine Suchfunktion, die die Suche erleichtert. Sie können auch in der Dokumentation Ihres SaaS-Client nachsehen, um die Einrichtung der Verbindung zu erleichtern.
3. Klicken Sie auf die Schaltfläche, um einen weiteren SAML-Identitätsanbieter hinzuzufügen.
4. Die meisten Services erfordern die Verwendung einer gemeinsamen Untergruppe der SAML-Felder. Geben Sie die erforderlichen Informationen in die Felder ein
5. Wenn Sie das IdP-Signaturzertifikat manuell einfügen, fügen Sie `----BEGIN-----` vor dem Zertifikattext und `----END CERTIFICATE-----` danach ein.
6. Klicken Sie auf den Befehl zum Speichern der Konfigurationsseite.

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 Dienstanbieter-Entity-ID 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 zuordnet, der von BlackBerry Enterprise Identity erkannt wird, beispielsweise ein Benutzername.
	  • Statisch – wenn Sie einen statischen Anspruch auswählen, müssen Sie eine Option im Attributwertefeld eingeben.
	• 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“.

6. Klicken Sie auf **Speichern**.

Erstellen eines SaaS-Dienstes in der BlackBerry Enterprise Identity-Konsole

1. Melden Sie sich bei der BlackBerry UEM-Administratorkonsole an und klicken Sie auf **Apps**.
2. Klicken Sie auf .
3. Klicken Sie auf das **Enterprise Identity**-Symbol.
4. Wenn Sie in einer Meldung aufgefordert werden, die Enterprise Identity-Cloud-Services zu synchronisieren, klicken Sie auf **Synchronisieren**.
5. Klicken Sie auf **Enterprise Identity-Konsole öffnen**.
6. Klicken Sie im linken Fensterbereich auf **Dienste**.
7. Wählen Sie in der Liste **Zu erstellenden Diensttyp auswählen** einen Service aus, und klicken Sie auf **+Erstellen**.
8. Füllen Sie die Felder entsprechend Ihrem SaaS-Dienstmandanten aus.

Name	Beschreibung
Zero Sign-On (ZSO, einmalige Anmeldung)	Wählen Sie diese Option aus, wenn Sie Zero Sign-On aktivieren möchten.
Name	Geben Sie den Namen des SaaS-Anbieters ein.
Beschreibung	Die Mandantenbeschreibung ist optional.
Entity-ID des Dienstanbieters	Geben Sie die URL oder einen eindeutigen Namen für den Zugriff auf den SaaS-Dienst ein.
Assertion Consumer Service URL	Geben Sie die vom Dienstanbieter bereitgestellte POST URL ein.

Name	Beschreibung
IdP-Signaturzertifikat	Geben Sie das mit dem Dienstanbieter gemeinsam genutzte x509-Zeritfikat ein.
IdP-Signaturschlüssel	Geben Sie den x509-Schlüssel für das entsprechende Signaturzertifikat ein. Bewahren Sie dieses sicher auf.
Dienstspezifische Informationen	Einige Dienste erfordern zusätzliche Information oder Informationen, die geringfügig von diesen Beschreibungen abweichen. Meistens sind diese Informationen jedoch bereits vorkonfiguriert.

9. Klicken Sie auf **Speichern**.
10. Klicken Sie auf **Aktivieren**.
11. Klicken Sie auf den von Ihnen erstellten Dienst.
12. Klicken Sie auf **Herunterladen**, um das Metadatendokument von der Enterprise Identity Administrationskonsole herunterzuladen.

Amazon Web Services-Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Amazon Web Services
Beschreibung	Amazon Web Services -Umgebung
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr
SAML-Anspruchsattribute	
Rolle	• Attribute = https://aws.amazon.com/SAML/Attributes/Role • Value = arn:aws:iam:<your_account_id>:role/SAML_admin_user,arn:aws:iam:<your_account_id>:saml-provider/<your_provider_name> • Typ = Statisch
Name der Rollensitzung	• Attribute = https://aws.amazon.com/SAML/Attributes/RoleSessionName • Wert = E-Mail-Adresse • Typ = Lokal

Weitere Informationen zum Einrichten der AWS-Dienstkonfiguration finden Sie in den Informationen von Amazon.

Box -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Box
Beschreibung	Box -Umgebung
Entity-ID des Dienstanbieters	box.net
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Citrix GoToMeeting -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	GoToMeeting
Beschreibung	GoToMeeting -Umgebung
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Concur -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Concur
Beschreibung	Concur -Umgebung
Entity-ID des Dienstanbieters	Aus Concur-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

DocuSign-Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	DocuSign
Beschreibung	DocuSign -Umgebung
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Dropbox -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Dropbox
Beschreibung	Dropbox -Umgebung
Entity-ID des Dienstanbieters	Aus Dropbox-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Egencia -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Egencia
Beschreibung	Egencia -Umgebung
Entity-ID des Dienstanbieters	Aus Egencia-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Evernote -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Evernote
Beschreibung	Evernote -Umgebung
Entity-ID des Dienstanbieters	Aus Evernote-Metadaten abrufen
Assertion Consumer Service URL	Aus Evernote-Metadaten abrufen
Signaturoptionen	Assertions und Gesamtantwort
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

G Suite -Dienstkonfiguration

Name	Beschreibung
Entity-ID des Dienstanbieters	google.com/a/domain
Assertion Consumer Service URL	https://www.google.com/a/<E-Mail-Domäne>/acs
Empfänger	https://www.google.com/a/<E-Mail-Domäne>/acs
Ziel	https://www.google.com/a/<E-Mail-Domäne>/acs
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Office 365 -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Office 365
Beschreibung	Microsoft Office 365 -Umgebung
Entity-ID des Identitätsanbieters	Enterprise-Identity-URL – Vanity-URL
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Einrichtung der Windows PowerShell

Jeder Microsoft Office 365-Mandant kann mehrere E-Mail-Domänen unterstützen. Vervollständigen Sie diese Schritte, um eine Microsoft Office 365-Domäne zu konfigurieren. Alle Microsoft Office 365-Befehle werden in Windows PowerShell ausgeführt.

Bevor Sie beginnen: Installieren Sie das Windows Management Framework 3.0. Dies beinhaltet Windows PowerShell. Details dazu finden Sie unter https://www.microsoft.com/en-us/download/details.aspx?id=34595.

1. Laden Sie sich das AzureActive Directory-Modul herunter und installieren Sie es. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/powershell/msonline/v1/azureactivedirectory?redirectedfrom=msdn#bkmk_installmodule.
2. Installieren Sie das Windows PowerShell-Modul für Skype. Dies finden Sie unter http://go.microsoft.com/fwlink/p/?LinkId=532439.
3. Starten Sie Windows PowerShell neu.
4. Richten Sie die folgenden Module unter Verwendung Ihrer Microsoft Office 365-Administratoranmeldedaten ein und authentifizieren Sie diese:
   a) Geben Sie `import-module MSOnline` ein. Drücken Sie die **Eingabetaste**.
   b) Geben Sie `$cred=Get-Credential` ein. Drücken Sie die **Eingabetaste**.
   c) Geben Sie `Connect-MsolService -Credential $cred` ein. Drücken Sie die **Eingabetaste**.

Hinzufügen einer neuen Microsoft Office 365-Domäne

Wenn Sie eine neue E-Mail-Domäne erstellen, müssen Sie auch eine neue Microsoft Office 365-Domäne erstellen.

Bevor Sie beginnen: Einrichtung der Windows PowerShell

1. Verwenden Sie Windows PowerShell, und geben Sie die folgenden Befehle ein, um ADAL für Microsoft Exchange Online zu aktivieren:
   a) `Set-ExecutionPolicy RemoteSigned`

b) `$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $cred -Authentication Basic -AllowRedirection`
c) `Import-PSSession $Session`
d) `Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true`
e) `Get-OrganizationConfig | ft name, *OAuth*`

2. Geben Sie in Windows PowerShell die folgenden Befehle ein:
   a) `Import-Module SkypeOnlineConnector`
   b) `$sfboSession = New-CsOnlineSession -Credential $cred`
   c) `Import-PSSession $sfboSession`
   d) `Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed`
   e) `Get-CsOAuthConfiguration`
3. Führen Sie in Windows PowerShell die folgenden Befehle aus, um eine neue Domäne hinzuzufügen. Ersetzen Sie Text in spitzen Klammern (< >) durch die Variablen, die zu Ihrer lokalen Umgebung passen. Es kann bis zu einer Stunde dauern, bis Änderungen an den Einstellungen wirksam werden.
4. Geben Sie `$domain = "<E-Mail-Serverdomäne>"` , wobei die E-Mail-Serverdomäne die Ihres E-Mail-Servers ist. Drücken Sie die **Eingabetaste**.
5. Verwenden Sie das in der Enterprise Identity-Servicekonfiguration für Microsoft Office 365 verwendete Zertifikat, und geben Sie Folgendes ein:`$certFile = "<Dateipfad cacert.pem>"`
6. Geben Sie `$cert = [IO.File]::ReadAllText($certFile)` ein. Drücken Sie die **Eingabetaste**.
7. Geben Sie `$cert = $cert.replace("-----BEGIN CERTIFICATE-----","")` ein. Drücken Sie die **Eingabetaste**.
8. Geben Sie `$cert = $cert.replace("-----END CERTIFICATE-----","")` ein. Drücken Sie die **Eingabetaste**.
9. Geben Sie `$cert = $cert.replace("`r","")` ein. Drücken Sie die **Eingabetaste**.
10. Geben Sie `$cert = $cert.replace("`n","")` ein. Drücken Sie die **Eingabetaste**.
11. Geben Sie `$activeLogOnUri = "https://idp.blackberry.com/<IDP-Vanity-URL oder Unternehmens-ID>/idp/profile/SAML2/SOAP/ECP/https%3A%2F%2Fidp.blackberry.com-<IDP-Vanity-URL oder Unternehmens-ID>"` ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.
12. Geben Sie `$brandName = "Enterprise ID"` ein. Drücken Sie die **Eingabetaste**.
13. Geben Sie `$issuerUri = "https://idp.blackberry.com-<IDP-Vanity-URL oder Unternehmens-ID>"` ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.
14. Geben Sie `$logOffUri = "https://idp.blackberry.com/<IDP-Vanity-URL oder Unternehmens-ID>/idp/profile/SAML2/Redirect/SLO/https%3A%2F%2Fidp.blackberry.com-<IDP-Vanity-URL oder Unternehmens-ID>"` ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.
15. Geben Sie `$passiveLogOnUri = "https://idp.blackberry.com/<IDP-Vanity-URL oder Unternehmens-ID>/idp/profile/SAML2/POST/SSO/https%3A%2F%2Fidp.blackberry.com-<IDP-Vanity-URL oder Unternehmens-ID>"` ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.
16. Geben Sie `$protocol = "SAMLP"` ein, und drücken Sie die **Eingabetaste**.
17. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication managed` ein. Drücken Sie die **Eingabetaste**.
18. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication federated -ActiveLogOnUri $activeLogOnUri -FederationBrandName $brandName -IssuerUri $issuerUri -LogOffUri $logOffUri -PassiveLogOnUri $passiveLogOnUri -`

`SigningCertificate $cert -PreferredAuthenticationProtocol $protocol` ein. Drücken Sie die **Eingabetaste**.

19. Prüfen Sie die Domäneneinstellungen mithilfe von `Get-MsolDomainFederationSEttings -DomainName $domain | Format-List *`.
20. Sind die Einstellungen richtig, schließen Sie Windows PowerShell. Um die Einstellungen zu bearbeiten, führen Sie die folgenden Befehle aus:
21. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication managed` ein. Drücken Sie die **Eingabetaste**.
22. Nehmen Sie die notwendigen Änderungen vor.
23. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication federated -ActiveLogOnUri $activeLogOnUri -FederationBrandName $brandName -IssuerUri $issuerUri -LogOffUri $logOffUri -PassiveLogOnUri $passiveLogOnUri -SigningCertificate $cert -PreferredAuthenticationProtocol $protocol` ein. Drücken Sie die **Eingabetaste**.

Aktualisieren einer bestehenden Microsoft Office 365-Domäne

Sie können bestehende Domänen aktualisieren, wenn die E-Mail-Domäne zu einer anderen Enterprise Identity-Domäne als Microsoft Office 365 weitergeleitet werden muss.

Bevor Sie beginnen: Einrichtung der Windows PowerShell

1. Führen Sie in Windows PowerShell die folgenden Befehle aus, um die vorhandene Domäne so zu ändern, dass sie auf die neue Domäne verweist.
2. Geben Sie `$domain = "<E-Mail-Serverdomäne>"` , wobei die E-Mail-Serverdomäne die Ihres E-Mail-Servers ist. Drücken Sie die **Eingabetaste**.
3. Um das in der Enterprise Identity-Servicekonfiguration für Microsoft Office 365 verwendete Zertifikat zu verwenden, geben Sie `$certFile = "<Dateipfad cacert.pem>"` ein. Drücken Sie die **Eingabetaste**.
4. Geben Sie `$cert = [IO.File]::ReadAllText($certFile)` ein. Drücken Sie die **Eingabetaste**.
5. Geben Sie `$cert = $cert.replace("-----BEGIN CERTIFICATE-----","")` ein. Drücken Sie die **Eingabetaste**.
6. Geben Sie `$cert = $cert.replace("-----END CERTIFICATE-----","")` ein. Drücken Sie die **Eingabetaste**.
7. Geben Sie `$cert = $cert.replace("`r","")` ein. Drücken Sie die **Eingabetaste**.
8. Geben Sie `$cert = $cert.replace("`n","")` ein. Drücken Sie die **Eingabetaste**.
9. Geben Sie `$activeLogOnUri = "https://idp.blackberry.com/<IDP-Vanity-URL oder Unternehmens-ID>/idp/profile/SAML2/SOAP/ECP/https%3A%2F%2Fidp.blackberry.com-<IDP-Vanity-URL oder Unternehmens-ID>"` ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.
10. Geben Sie `$brandName = "Enterprise ID"` ein. Drücken Sie die **Eingabetaste**.
11. Geben Sie `$issuerUri = "https://idp.blackberry.com-<IDP-Vanity-URL oder Unternehmens-ID>"` ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.
12. Geben Sie `$logOffUri = "https://idp.blackberry.com/<IDP-Vanity-URL oder Unternehmens-ID>/idp/profile/SAML2/Redirect/SLO/https%3A%2F%2Fidp.blackberry.com-<IDP-Vanity-URL oder Unternehmens-ID>"` ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.
13. Geben Sie `$passiveLogOnUri = "https://idp.blackberry.com/<IDP-Vanity-URL oder Unternehmens-ID>/idp/profile/SAML2/POST/SSO/https%3A%2F%2Fidp.blackberry.com-`

<*IDP-Vanity-URL oder Unternehmens-ID*>" ein, wobei die *IDP-Vanity-URL oder Unternehmens-ID* der Vanity-URL bzw. Unternehmens-ID entspricht. Drücken Sie die **Eingabetaste**.

14. Geben Sie `$protocol = "SAMLP“` ein. Drücken Sie die **Eingabetaste**.
15. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication managed` ein. Drücken Sie die **Eingabetaste**.
16. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication federated -ActiveLogOnUri $activeLogOnUri -FederationBrandName $brandName -IssuerUri $issuerUri -LogOffUri $logOffUri -PassiveLogOnUri $passiveLogOnUri -SigningCertificate $cert -PreferredAuthenticationProtocol $protocol` ein. Drücken Sie die **Eingabetaste**.
17. Prüfen Sie die Domäneneinstellungen mithilfe von `Get-MsolDomainFederationSEttings -DomainName $domain | Format-List *`.
18. Sind die Einstellungen richtig, schließen Sie Windows PowerShell. Um die Einstellungen zu bearbeiten, verwenden Sie die folgenden Befehle:
19. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication managed` ein. Drücken Sie die **Eingabetaste**.
20. Nehmen Sie die notwendigen Änderungen vor.
21. Geben Sie `Set-MsolDomainAuthentication -DomainName $domain -Authentication federated -ActiveLogOnUri $activeLogOnUri -FederationBrandName $brandName -IssuerUri $issuerUri -LogOffUri $logOffUri -PassiveLogOnUri $passiveLogOnUri -SigningCertificate $cert -PreferredAuthenticationProtocol $protocol` ein. Drücken Sie die **Eingabetaste**.

Salesforce -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Salesforce
Beschreibung	Salesforce -Umgebung
Entity-ID des Dienstanbieters	Aus Salesforce-Metadaten abrufen
Assertion Consumer Service URL	Aus Salesforce-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

ServiceNow -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	ServiceNow
Beschreibung	ServiceNow -Umgebung
Entity-ID des Dienstanbieters	Aus ServiceNow-Metadaten abrufen
Assertion Consumer Service URL	Aus ServiceNow-Metadaten abrufen
Service-URL für einmalige Abmeldung	ServiceNow -Umgebung
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

WebEx -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	WebEx
Beschreibung	Cisco WebEx -Umgebung
Entity-ID des Dienstanbieters	Aus WebEx-Metadaten abrufen
Assertion Consumer Service URL	Aus WebEx-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

WebFOCUS-Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	WebFOCUS
Beschreibung	WebFOCUS -Umgebung
Entity-ID des Dienstanbieters	Aus WebFOCUS-Metadaten abrufen
Assertion Consumer Service URL	Aus WebFOCUS-Metadaten abrufen
Vom Dienstanbieter ausgehende Anmelde-URL	Aus WebFOCUS-Metadaten abrufen
Service-URL für einmalige Abmeldung	Aus WebFOCUS-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Workday -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Workday
Beschreibung	Workday -Umgebung
Entity-ID des Dienstanbieters	Aus Workday-Metadaten abrufen
Assertion Consumer Service URL	Aus Workday-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Workspaces-Dienstkonfiguration

Single Sign-On für Workspaces zur Kompatibilität mit einer firmeninternen Instanz von BlackBerry UEM

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Workspaces
Beschreibung	Workspaces -Umgebung
Entity-ID des Dienstanbieters	com.watchdox.saml
Von Dienstanbieter bereitgestellte Anmelde-URL	Aus Workspaces-Metadaten abrufen
Aussteller	Aus Workspaces-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Konfigurieren von BlackBerry Enterprise Identity zur Kompatibilität mit Workspaces

Bevor Sie beginnen: Sie müssen über die folgende Umgebung verfügen:

- eine firmeninterne Installation von Workspaces mit vApp oder Appliance-X
- einen BlackBerry UEM-Server oder eine BlackBerry UEM Cloud-Instanz, für die Enterprise Identity aktiviert ist

Hinweis:

Neue BlackBerry UEM Cloud- und Workspaces-Mandanten werden jetzt automatisch so konfiguriert, dass Benutzer sich bei Enterprise Identity anmelden können, was die Anwendung von Zwei-Faktor-Authentifizierung oder anderen erweiterten Zugriffsrichtlinien ermöglicht (bereits bestehende BlackBerry UEM Cloud-Mandanten erhalten diese Möglichkeit in einer zukünftigen Version)

1. Navigieren Sie zu `https://<your server>/saml-idp/saml/metadata`.
2. Laden Sie die Metadatendatei herunter.
3. Erstellen Sie ein Lizenzschlüsselpaar.
4. Führen Sie einen der folgenden Schritte aus:
   - Verwenden Sie die BlackBerry UEM-Verwaltungskonsole Version 12.6.3 oder früher, um sich bei der Enterprise Identity-Konsole anzumelden.
   - Verwenden Sie die BlackBerry UEM-Verwaltungskonsole Version 12.7 oder höher, oder die BlackBerry UEM Cloud-Verwaltungskonsole, um sich bei der Enterprise Identity-Konsole anzumelden.
5. Erstellen Sie einen Workspaces-Dienst.
6. Ordnen Sie die Dienstentitäts-ID und die Anmelde-/Abmelde-URL aus den Metadaten den entsprechenden Feldern im Workspaces-Dienst zu.

7. Konfigurieren Sie mit dem zuvor erstellten Schlüsselpaar das IDP-Signaturzertifikat und den privaten Schlüssel.
8. Legen Sie den Anspruch als `E-Mail-Adresse (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresses)` fest.
9. Klicken Sie auf **Speichern**.
10. Laden Sie die Metadaten für den Workspaces-Dienst herunter.
11. Melden Sie sich mit einem Administratorkonto bei der Workspaces-Verwaltungskonsole an.
12. Klicken Sie auf **Authentifizierungstyp**, und wählen Sie **BlackBerry Enterprise Identity** aus.
13. Laden Sie die aus BlackBerry UEM heruntergeladenen Metadaten für Workspaces hoch. Dadurch wird ein neuer IDP in Workspaces erstellt.
14. Klicken Sie auf **Speichern**.
15. Melden Sie sich beim WorkspacesBlackBerry Workspaces Configuration Tool an, und verknüpfen Sie den Mandanten mit dem neuen IDP.
16. Melden Sie sich bei der Workspaces-URL an, und stellen Sie sicher, dass diese Sie zum IDP weiterleitet.
17. Stellen Sie sicher, dass alles ordnungsgemäß funktioniert, indem Sie den Benutzernamen und das Kennwort für einen Benutzer eingeben, der für BlackBerry Enterprise Identity aktiviert wurde.

Yammer-Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Yammer
Beschreibung	Yammer-Umgebung
Entity-ID des Dienstanbieters	Aus Yammer-Metadaten abrufen

Zendesk -Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Zendesk
Beschreibung	Zendesk -Umgebung
Entity-ID des Dienstanbieters	Aus Zendesk-Metadaten abrufen
Assertion Consumer Service URL	Aus Zendesk-Metadaten abrufen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Zscaler-Dienstkonfiguration

Name	Beschreibung
Mobile ZSO	Wählen Sie diese Option aus, wenn Sie das Mobile ZSO aktivieren möchten.
Name	Zscaler
Beschreibung	Zscaler-Umgebung
Entity-ID des Dienstanbieters	Aus Zscaler-Metadaten abrufen
Assertion Consumer Service URL	Aus Zscaler-Metadaten abrufen
Von Dienstanbieter bereitgestellte Anmelde-URL	URL für geschützte Ressourcen
Signaturzertifikat	Wahr
Signaturschlüssel	Wahr

Rechtliche Hinweise

©2018 BlackBerry Limited. Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

Amazon Web Services ist eine Marke von Amazon.com, Inc. oder seinen angegliederten Unternehmen in den USA und/oder anderen Ländern. Android und Google Chrome are trademarks of Google Inc. Box ist eine Marke, Dienstleistungsmarke oder eingetragene Marke von Box, Inc. Concur ist eine Marke von OpenVPN Technologies, Inc. DocuSign is a trademark of DocuSign, Inc. in the United States and/or other countries. Dropbox ist eine Marke der Dropbox, Inc. Egencia ist eine Marke von Egencia LLC. Evernote ist eine Marke von Evernote Corporation. ist eine Marke von Cisco Systems, Inc. und/oder seiner angegliederten Unternehmen in den USA und einigen anderen Ländern. iOS® wird unter Lizenz von Apple Inc. verwendet. Linux ist eine Marke von Linus Torvalds. Mac OS und Safari sind Marken von Apple Inc. Microsoft, Active Directory und Internet Explorer sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Mozilla und Firefox sind Marken der Mozilla Foundation. OpenSSL ist eine Marke der The OpenSSL Software Foundation, Inc. Oracle VM VirtualBox ist eine Marke von Oracle und/oder seiner angegliederten Unternehmen. Salesforce ist eine Marke von salesforce.com, Inc. und wird hier mit entsprechender Genehmigung verwendet. ServiceNow Ubuntu ist eine Marke von ServiceNow. ist eine Marke von Canonical Limited. WebFOCUS ist eine Marke von Information Builders, Inc. Workday ist eine Marke der Workday, Inc. Zendeskis a trademark of Zendesk, Inc. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

Dieses Dokument und alle Dokumente, die per Verweis in dieses Dokument mit einbezogen werden, z. B. alle über die BlackBerry-Webseite erhältlichen Dokumente, werden ohne Mängelgewähr und je nach Verfügbarkeit bereitgestellt. Die entsprechenden Dokumente werden ohne ausdrückliche Billigung, Gewährleistung oder Garantie seitens BlackBerry Limited und seinen angegliederten Unternehmen („BlackBerry“) bereitgestellt. BlackBerry übernimmt keine Verantwortung für eventuelle typografische, technische oder anderweitige Ungenauigkeiten sowie für Fehler und Auslassungen in den genannten Dokumenten. Die BlackBerry-Technologie ist in dieser Dokumentation teilweise in verallgemeinerter Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von BlackBerry zu schützen. BlackBerry behält sich das Recht vor, die in diesem Dokument enthaltenen Informationen von Zeit zu Zeit zu ändern. BlackBerry ist jedoch nicht verpflichtet, die Benutzer über diese Änderungen, Updates, Verbesserungen oder Zusätze rechtzeitig bzw. überhaupt in Kenntnis zu setzen.

Diese Dokumentation enthält möglicherweise Verweise auf Informationsquellen, Hardware oder Software, Produkte oder Dienste, einschließlich Komponenten und Inhalte wie urheberrechtlich geschützte Inhalte und/oder Websites von Drittanbietern (nachfolgend "Drittprodukte und -dienste" genannt). BlackBerry hat keinen Einfluss auf und übernimmt keine Haftung für Drittprodukte und -dienste, dies gilt u. a. für Inhalt, Genauigkeit, Einhaltung der Urheberrechtsgesetze, Kompatibilität, Leistung, Zuverlässigkeit, Rechtmäßigkeit, Schicklichkeit, Links oder andere Aspekte der Drittprodukte und -dienste. Der Einschluss eines Verweises auf Drittprodukte und -dienste in dieser Dokumentation impliziert in keiner Weise eine besondere Empfehlung der Drittprodukte und -dienste oder des Drittanbieters durch BlackBerry.

SOFERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDEN QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, USANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER

DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDEN LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTANBIETER-PRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE HABEN SIE ZUDEM ANDERE LANDESSPEZIFISCHE RECHTE. IN MANCHEN RECHTSGEBIETEN IST DER AUSSCHLUSS ODER DIE EINSCHRÄNKUNG KONKLUDENTER GEWÄHRLEISTUNGEN UND BEDINGUNGEN NICHT ZULÄSSIG. IN DEM GESETZLICH ZULÄSSIGEN UMFANG WERDEN SÄMTLICHE KONKLUDENTEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN IM ZUSAMMENHANG MIT DER DOKUMENTATION, DIE EINGESCHRÄNKT WERDEN KÖNNEN, SOFERN SIE NICHT WIE OBEN 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, VERLUSTES GESCHÄFTLICHER DATEN, ENTGANGENER GESCHÄFTSCHANCEN ODER BESCHÄDIGUNG BZW. VERLUSTES VON DATEN, DES UNVERMÖGENS, DATEN ZU ÜBERTRAGEN ODER ZU EMPFANGEN, PROBLEMEN 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 AIRTIME-DIENSTEN, 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 AIRTIME-DIENSTANBIETERN), AUTORISIERTE BLACKBERRY-DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH AIRTIME-DIENSTANBIETERN) 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 BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem Dienstanbieter bezüglich Verfügbarkeit, Roaming-Vereinbarungen, Service-Plänen 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 behandelt wird.

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE DER IN DIESER DOKUMENTATION DARGELEGTEN BESTIMMUNGEN SETZEN IRGENDWELCHE AUSDRÜCKLICHEN SCHRIFTLICHEN VEREINBARUNGEN ODER GEWÄHRLEISTUNGEN VON BLACKBERRY FÜR TEILE VON BLACKBERRY-PRODUKTEN ODER -DIENSTEN AUSSER KRAFT.

BlackBerry Enterprise Software umfasst spezifische Drittanbietersoftware. Die Lizenz und Copyright-Informationen für diese Software sind verfügbar unter: http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Veröffentlicht in Kanada