



# **BlackBerry 2FA**

## **Handbuch zur Serverkonfiguration**

3.4



# Inhalt

<b>Schritte beim Konfigurieren des BlackBerry 2FA-Servers.....</b>	<b>5</b>
<b>Konfigurieren einer Verbindung zwischen dem BlackBerry 2FA-Server und einem VPN-Gateway.....</b>	<b>6</b>
Unterstützte Authentifizierungsprotokolle für die einzelnen Authentifizierungsoptionen.....	6
Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf einem Cisco ASA Series-VPN-Gateway.....	7
Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf Citrix NetScaler.....	8
Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf F5 BIG-IP.....	8
Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf einem Barracuda-SSL-VPN.....	9
Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf einem strongSwan-Server.....	9
Konfigurieren des BlackBerry 2FA-Servers für die Verbindung mit einem VPN-Gateway.....	11
Aktualisieren einer Verbindung zu einem VPN-Gateway.....	12
Löschen einer Verbindung zu einem VPN-Gateway.....	12
<b>Konfigurieren der Verbindung zum REST-API-Endpunkt.....</b>	<b>13</b>
Konfigurieren der REST-API-Endpunktkonnektivität.....	13
<b>Erstellen eines REST-API-Client im BlackBerry 2FA-Server.....</b>	<b>15</b>
<b>Aktivieren der MS-CHAP-Authentifizierung für Benutzer in einer Domäne.....</b>	<b>16</b>
<b>Konfigurieren der BlackBerry 2FA-App.....</b>	<b>17</b>
<b>Zuordnen eines VPN-Gateways oder einer REST-Client-Konfiguration zu einer Benutzergruppe.....</b>	<b>18</b>
<b>Installieren der BlackBerry 2FA-App auf Geräten.....</b>	<b>19</b>
<b>Architektur: Hohe Verfügbarkeit für BlackBerry 2FA.....</b>	<b>20</b>
Konfigurieren des BlackBerry 2FA-Servers für hohe Verfügbarkeit.....	20
<b>Protokollierung und Reporting.....</b>	<b>22</b>
Überwachung von Authentifizierungsanforderungen.....	22
Zentralisieren von Protokollierungs- oder Überwachungsvorgängen mit Syslog.....	23

<b>Authentifizierungsoptionen.....</b>	<b>26</b>
<b>Benutzernamen, Kennwörter und Verzeichnisse.....</b>	<b>28</b>
<b>REST-API-Endpunkt.....</b>	<b>30</b>
<b>VPN-Gateways.....</b>	<b>31</b>
<b>Glossar.....</b>	<b>32</b>
<b>Rechtliche Hinweise.....</b>	<b>34</b>

# Schritte beim Konfigurieren des BlackBerry 2FA-Servers

Zum Konfigurieren des BlackBerry 2FA-Servers führen Sie die folgenden Aktionen aus:

Aufgabe	Beschreibung
1	Laden Sie bei Bedarf den BlackBerry 2FA-Server herunter und installieren Sie ihn. Nachdem Sie den Server installiert haben, müssen Sie eine Aktivierungsdatei generieren und herunterladen, um die Kommunikation zwischen dem BlackBerry 2FA-Server und BlackBerry UEM zu ermöglichen. Weitere Informationen finden Sie in der <a href="#">Dokumentation zu Installation und Upgrade von BlackBerry 2FA-Servern</a> .
2	Erstellen Sie auf dem VPN-Server ein Profil für den BlackBerry 2FA-Server. Weitere Informationen finden Sie unter <a href="#">Konfigurieren einer Verbindung zwischen dem BlackBerry 2FA-Server und einem VPN-Gateway</a> .
3	Konfigurieren des BlackBerry 2FA-Servers für die Verbindung mit einem VPN-Gateway
4	Konfigurieren der Verbindung zum REST-API-Endpoint
5	Erstellen eines REST-API-Client im BlackBerry 2FA-Server
6	Aktivieren der MS-CHAP-Authentifizierung für Benutzer in einer Domäne
7	Konfigurieren der BlackBerry 2FA-App
8	Zuordnen eines VPN-Gateways oder einer REST-Client-Konfiguration zu einer Benutzergruppe
9	Senden Sie die BlackBerry 2FA-App bei Bedarf an die entsprechenden Geräte. Weitere Informationen finden Sie unter <a href="#">Installieren der BlackBerry 2FA-App auf Geräten</a> .

# Konfigurieren einer Verbindung zwischen dem BlackBerry 2FA-Server und einem VPN-Gateway

Der BlackBerry 2FA-Server muss auf Ihrem VPN-Server als ein RADIUS-Server konfiguriert sein, an den Authentifizierungsanforderungen weitergeleitet werden. Der BlackBerry 2FA-Server führt folgende Aufgaben durch, um Benutzer für die Verbindung mit einem VPN-Gateway zu authentifizieren:

- Authentifizierung des Geräts oder des Einmalkennworts (OTP) des Benutzers
- Es fungiert als ein Proxy für die Kennwortauthentifizierung.
- Es kombiniert zwei Ergebnisse, um zu ermitteln, ob die Authentifizierung erfolgreich verläuft.

Sie müssen auch ein VPN-Client-Profil oder einen Client konfigurieren, der Benutzern die Auswahl von BlackBerry 2FA erlaubt, wenn sich diese über ihre Computer am VPN anmelden.

Für den RADIUS-Server müssen für sämtliche BlackBerry 2FA-Server in Ihrer Umgebung folgende Optionen eingestellt sein:

- IP-Adresse oder FQDN des Computers, der den BlackBerry 2FA-Server hostet
- Timeout zwischen 60 und 90 Sekunden für die Verbindung zwischen dem VPN-Server und dem BlackBerry 2FA-Server
- Gemeinsamen geheimen Schlüssel
- Für den Authentifizierungsport 1812 festlegen
- Je nach verfügbaren Authentifizierungsoptionen eine der folgenden Optionen: PAP, MS-CHAP v1, MS-CHAP v2 oder EAP-MSCHAP

Für das VPN-Client-Profil muss das Timeout zwischen 30 und 60 Sekunden für die Verbindung zwischen dem VPN-Client auf den Computern des Benutzers und dem VPN-Server festgelegt sein.

Anweisungen zum Konfigurieren eines RADIUS-Servers oder eines VPN-Client-Profiles finden Sie in der Dokumentation des VPN-Servers, den Sie verwenden.

Eine Liste der unterstützten VPN-Server finden Sie in der [BlackBerry 2FA-Dokumentation zur Server-Kompatibilitätsmatrix](#).

## Unterstützte Authentifizierungsprotokolle für die einzelnen Authentifizierungsoptionen

In der folgenden Tabelle sind die Authentifizierungsprotokolle aufgeführt, die für jede von BlackBerry 2FA unterstützte Authentifizierungsoption verfügbar sind.

**Hinweis:** Wenn Ihre Benutzer sich mit OTP-Token (Token für Einmalkennwörter) authentifizieren, muss der VPN-Server für die Authentifizierung mit PAP konfiguriert sein. OTPs werden nicht zusammen mit MSCHAPv1, MSCHAPv2 oder EAP-MSCHAP unterstützt.

Authentifizierungsoption	Unterstützte Authentifizierungsprotokolle
Zwei-Faktor-Authentifizierung mit passivem Gerätekennwort	PAP
Zwei-Faktor-Authentifizierung mit aktivem Gerätekennwort	PAP

Authentifizierungsoption	Unterstützte Authentifizierungsprotokolle
Zwei-Faktor-Authentifizierung mittels Unternehmenskennwort	MS-CHAP v1, MS-CHAP v2, PAP, EAP-MSCHAP
Ein-Faktor-Authentifizierung mittels Unternehmenskennwort	MS-CHAP v1, MS-CHAP v2, PAP, EAP-MSCHAP

## Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf einem Cisco ASA Series-VPN-Gateway

Wenn Sie ein Cisco ASA Series-VPN-Gateway verwenden, können Sie das VPN-Profil mithilfe der nachstehenden Informationen erstellen.

Detaillierte Anweisungen zum Konfigurieren des VPN-Profiles finden Sie unter <http://www.cisco.com> in der Cisco ASA Series-Dokumentation.

Wenn Sie das Profil erstellen, müssen Sie zur Unterstützung von BlackBerry 2FA die folgenden Optionen einrichten:

- Erstellen Sie für jeden BlackBerry 2FA-Server in Ihrer Umgebung eine RADIUS-AAA-Servergruppe mit folgenden Optionen:
  - IP-Adresse oder FQDN des Computers, der den BlackBerry 2FA-Server hostet
  - Timeout zwischen 60 und 90 Sekunden für die Verbindung zwischen dem VPN-Gateway und dem BlackBerry 2FA-Server
  - Gemeinsamen geheimen Schlüssel
  - Für den Authentifizierungsport 1812 festlegen
  - Kompatibilität mit MS-CHAP v2
- Legen Sie das Timeout für die Verbindung zwischen dem VPN-Client auf Computern von Benutzern und dem VPN-Gateway auf 30 bis 60 Sekunden fest. Sie müssen das Timeout in der Profildatei des Cisco AnyConnect-VPN-Client (eine XML-Datei) konfigurieren, die auf den Computern von Benutzer installiert sein muss.
- Kennwortverwaltungsoption, wenn Sie das Profil zur Unterstützung der MS-CHAP-v2-Authentifizierung konfigurieren

Um die Profilerstellung abzuschließen, müssen Sie die folgenden Schritte ausführen:

- Das VPN-TPE-Protokoll (Tunnel Payload Encapsulation) aktivieren (z. B. das IPSEC-IKE-v2-Protokoll)
- Alle Befehle, die für die zugehörige VPN-Richtliniengruppe erforderlich sind
- Sämtliche Befehle, die für das zugehörige Cisco AnyConnect-VPN-Client-Profil und die Erstellung der XML-Datei an sich nötig sind
- Alle Befehle, die für die zugehörige VPN-Tunnelgruppe erforderlich sind

Sie müssen keine zusätzliche Zertifikatauthentifizierung konfigurieren.

Wenn Sie auf dem BlackBerry 2FA-Server die VPN-Gateway-Verbindung konfigurieren, müssen Sie den gemeinsamen geheimen RADIUS-Schlüssel angeben, den Sie im VPN-Profil festlegen.

## Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf Citrix NetScaler

Wenn Sie Citrix NetScaler verwenden, können Sie die Verbindung zum BlackBerry 2FA-Server konfigurieren, indem Sie ihn als RADIUS-Server hinzufügen. Wenn Sie mehrere BlackBerry 2FA-Server in Ihrer Umgebung haben, müssen Sie für jeden Server einen separaten RADIUS-Server konfigurieren.

Detaillierte Anweisungen zum Konfigurieren der Verbindung von NetScaler zum BlackBerry 2FA-Server finden Sie unter <http://docs.citrix.com/en-us/netscaler.html> im Abschnitt „Configuring RADIUS Authentication“ in der NetScaler-Systemdokumentation.

Sie können beispielsweise eine Verbindung zu einem BlackBerry 2FA-Server konfigurieren und BlackBerry 2FA als Standardauthentifizierungsmethode verwenden. Wenn Sie dieses Beispiel konfigurieren möchten, müssen Sie im Konfigurationsprogramm für NetScaler die Authentifizierungseinstellungen in den globalen Einstellungen wie folgt festlegen:

- „Maximum Number of Users“, „Max Login Attempts“ und „Failed Login Timeout“, je nach den Anforderungen Ihres Unternehmens.
- Authentifizierungstyp auf RADIUS festlegen
- IP-Adresse auf den BlackBerry 2FA-Server festlegen
- Für den Port 1812 festlegen
- Timeout zwischen 60 und 90 Sekunden für die Verbindung zwischen NetScaler und dem BlackBerry 2FA-Server
- Gemeinsamen geheimen Schlüssel
- „Enable NAS IP address extraction“ auswählen
- „Password Encoding“ muss auf das Authentifizierungsprotokoll festgelegt werden, das die von Ihnen ausgewählte VPN-Authentifizierungsoption unterstützt (BlackBerry 2FA unterstützt nicht die Option „chap“).
- Für „Accounting“ den Wert „Off“ festlegen

## Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf F5 BIG-IP

Wenn Sie F5 BIG-IP mit einem AAA-Server verwenden, können Sie mit dem Access Policy Manager unter Verwendung der folgenden Informationen eine Zugriffsrichtlinie erstellen.

Detaillierte Anweisungen zum Konfigurieren der Authentifizierung mithilfe von AAA-Servern finden Sie unter [https://support.f5.com/kb/en-us/products/big-ip\\_apm/manuals/product/apm\\_config\\_10\\_2\\_0/apm\\_config\\_server\\_auth.html](https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm_config_10_2_0/apm_config_server_auth.html) in der F5BIG-IP-Dokumentation.

Wenn Sie die Richtlinie erstellen, müssen Sie zur Unterstützung von BlackBerry 2FA die folgenden Optionen einrichten:

- RADIUS als Authentifizierungstyp festlegen
- die IP-Adresse oder FQDN des Computers festlegen, der den BlackBerry 2FA-Server hostet
- ein Timeout zwischen 60 und 90 Sekunden für die Verbindung zwischen dem VPN-Gateway und dem BlackBerry 2FA-Server konfigurieren
- einen gemeinsamen geheimen Schlüssel festlegen
- für den Authentifizierungsport 1812 festlegen
- überprüfen, ob MS-CHAP v2 unterstützt wird
- „Accounting“ ausschalten
- die maximale Anzahl von Anmeldeversuchen festlegen



Die Richtlinie muss jedem BlackBerry 2FA-Server in Ihrer Umgebung zugewiesen sein.

## Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf einem Barracuda-SSL-VPN

Wenn Sie ein Barracuda-SSL-VPN verwenden, können Sie die Verbindung zum BlackBerry 2FA-Server konfigurieren, indem Sie ihn als RADIUS-Server hinzufügen. Wenn Sie mehrere BlackBerry 2FA-Server in Ihrer Umgebung haben, müssen Sie für jeden Server einen separaten RADIUS-Server konfigurieren.

Detaillierte Anweisungen zum Konfigurieren des Barracuda-SSL-VPN zur Verbindung mit dem BlackBerry 2FA-Server finden Sie unter <https://www.barracuda.com/support/knowledgebase/5016000000HZG9AAO>.

Sie müssen einen RADIUS-Server mit den folgenden Optionen konfigurieren, damit BlackBerry 2FA unterstützt wird:

- RADIUS als Authentifizierungstyp festlegen
- die IP-Adresse oder FQDN des Computers festlegen, der den BlackBerry 2FA-Server hostet
- ein Timeout zwischen 60 und 90 Sekunden für die Verbindung zwischen dem VPN-Gateway und dem BlackBerry 2FA-Server konfigurieren
- einen gemeinsamen geheimen Schlüssel festlegen
- für den Authentifizierungsport 1812 festlegen
- überprüfen, ob MS-CHAP v2 unterstützt wird
- „Accounting“ ausschalten
- die maximale Anzahl von Anmeldeversuchen festlegen

## Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf einem strongSwan-Server

Zum Konfigurieren der Verbindung zum BlackBerry 2FA-Server auf einem strongSwan-Server müssen Sie die Dateien ipsec.conf und eap-radius.conf ändern.

Weitere Informationen zu diesen Dateien und zum Konfigurieren von strongSwan finden Sie unter [visit https://www.strongswan.org/](https://www.strongswan.org/).

### Konfiguration von ipsec.conf

Die Datei ipsec.conf befindet sich im Verzeichnis /etc. Sie müssen einen neuen Abschnitt „conn“ für den BlackBerry 2FA-Server hinzufügen. Beispiel:

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

Einstellung	Beschreibung
<Name>	Das ist ein eindeutiger Name für den neuen Verbindungsabschnitt. Es ist eine gängige Praxis, dass dieser Name einige wichtige Merkmale der Verbindung selbst enthält (z. B. IPSec-IKEv2-radius).
keyexchange=ikev2	Mit dieser Einstellung werden Schlüsselaustauschmethoden festgelegt (z. B. IKEv1, IKEv2). Der BlackBerry 2FA-Server verwendet diese Einstellung nicht, aber Sie müssen diese im Abschnitt „conn“ aufnehmen, um einen ordnungsgemäßen Schlüsselaustausch mit VPN-Clients zu ermöglichen. Sie müssen sicherstellen, dass die VPN-Clients, die mit dem strongSwan-Server verbunden sind, dieselbe Methode für den Schlüsselaustausch nutzen.
rightauth=eap-radius	Diese Einstellung gibt vor, dass der strongSwan-Server EAP anstelle von RADIUS zur Authentifizierung von VPN-Clients für diese Art der Verbindung verwendet.
rightsendsert=never	Diese Einstellung gibt vor, dass Benutzerzertifikate nicht für die Client-Authentifizierung verwendet werden.
eap_identity=%any	Diese Einstellung gibt die Identität des VPN-Clients an, der für die Authentifizierung zu verwenden ist. Der BlackBerry 2FA-Server verwendet diese Einstellung nicht, aber Sie müssen diese im Abschnitt „conn“ aufnehmen. Der Wert „%any“ weist den strongSwan-Server an, die vom VPN-Client bereitgestellte Identität zu übergeben.
auto=add	Diese Einstellung gibt an, dass dieser Verbindungsabschnitt aktiv ist. Der BlackBerry 2FA-Server verwendet diese Einstellung nicht, aber Sie müssen diese im Abschnitt „conn“ aufnehmen.

### Konfiguration von eap-radius.conf

Die Datei eap-radius.conf befindet sich im Verzeichnis /etc/strongswan.d/charon. Sie enthält die 'Details zur Verwendung von EAP anstelle von RADIUS für die Authentifizierung. Die Standardkonfigurationsdatei enthält alle Einstellungen, die Sie konfigurieren müssen, die meisten davon sind jedoch auskommentiert, und einigen ist gar kein Wert zugewiesen. Sie müssen die erforderlichen Einstellungen ändern, indem Sie das Rautezeichen (#) entfernen und deren Werte wie in der nachfolgenden Tabelle beschrieben festlegen.

Einstellung	Beschreibung
accounting=no	Diese Einstellung verhindert, dass strongSwan RADIUS-Accounting-Informationen an den BlackBerry 2FA-Server sendet.
nas_identifier	Diese optionale Einstellung gibt an, dass der NAS-Identifikator in RADIUS-Nachrichten aufgenommen werden soll. Sie können diese Einstellung verwenden, wenn mehrere strongSwan-Server denselben BlackBerry 2FA-Server verwenden.
port=1812	Diese Einstellung gibt den Port an, den der BlackBerry 2FA-Server für den Empfang von RADIUS-Authentifizierungsanforderungen verwendet.

Einstellung	Beschreibung
secret=<Gemeinsamer geheimer Schlüssel>	In dieser Einstellung wird der gemeinsame geheime Schlüssel zwischen strongSwan- und BlackBerry 2FA-Server festgelegt. Wenn Sie auf dem BlackBerry 2FA-Server die VPN-Serververbindung konfigurieren, müssen Sie den gemeinsamen geheimen RADIUS-Schlüssel eingeben, den Sie hier festlegen.
server=<IP des VPNAuth-Servers>	Diese Einstellung legt die IP-Adresse oder FQDN des BlackBerry 2FA-Servers fest.
ike_to_radius=1, 2, 311:1, 311:11, 311:25	<p>Mit dieser Einstellung wird eine durch Komma getrennte Liste von Ziffern festgelegt, welche die Liste der RADIUS-Attribute darstellt, die strongSwan an den BlackBerry 2FA-Server weiterleiten muss.</p> <p>Bei durch Doppelpunkt getrennten Ziffern handelt es sich um anbieterspezifische Attribute. Die erste Zahl identifiziert den Anbieter (311 ist beispielsweise die Zahl für Microsoft), und die zweite Zahl identifiziert den Attributtyp.</p> <p>Diese Einstellung ist im Abschnitt „forward“ der Konfigurationsdatei enthalten.</p>
radius_to_ike=311:26, 311:17, 311:16	<p>Mit dieser Einstellung wird eine durch Komma getrennte Liste von Ziffern festgelegt, welche die Liste der RADIUS-Attribute darstellt, die der BlackBerry 2FA-Server an strongSwan weiterleiten muss.</p> <p>Bei durch Doppelpunkt getrennten Ziffern handelt es sich um anbieterspezifische Attribute. Die erste Zahl identifiziert den Anbieter (311 ist beispielsweise die Zahl für Microsoft), und die zweite Zahl identifiziert den Attributtyp.</p> <p>Diese Einstellung ist im Abschnitt „forward“ der Konfigurationsdatei enthalten.</p>

## Konfigurieren des BlackBerry 2FA-Servers für die Verbindung mit einem VPN-Gateway

**Bevor Sie beginnen:** Rufen Sie die IP-Adresse und den gemeinsamen geheimen Schlüssel für die VPN-Gateways ab.


1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry 2FA-Server**.
2. Klicken Sie auf den BlackBerry 2FA-Server, für den Sie ein VPN-Gateway konfigurieren möchten.
3. Klicken Sie im Abschnitt **VPN-Konfiguration** auf **+**.
4. Geben Sie im Feld **Name des VPN-Servers** einen eindeutigen Namen für das VPN-Gateway ein, mit dem Sie eine Verbindung herstellen möchten.
5. Geben Sie im Feld **VPN-Host** die IP-Adresse des VPN-Gateways ein.
6. Geben Sie in den Feldern **Gemeinsamer geheimer Schlüssel** und **Geheimen Schlüssel bestätigen** den gemeinsamen geheimen Schlüssel des VPN-Gateways ein und bestätigen Sie diesen.

7. Überschreiben Sie optional die BlackBerry 2FA-Appkonfiguration. Die folgenden Felder können Sie unabhängig voneinander konfigurieren. Leer Felder bleiben unberücksichtigt, stattdessen werden die Werte des Abschnitts **Standardgeräteaufforderung** verwendet.
  - a) Wählen Sie **BlackBerry 2FA-Eingabeaufforderung für dieses VPN** aus.
  - b) Geben Sie im Feld **Titel** den Titel an, der in der Nachricht der App angezeigt werden soll. Beispielsweise „VPN des Beispielunternehmens“.
  - c) Geben Sie im Feld **Nachricht** die Nachricht ein, die die App Benutzern anzeigen soll. In dieser Nachricht wird Benutzern erklärt, was von ihnen benötigt wird.
  - d) Geben Sie im Feld **Schaltflächentext bestätigen** den Text ein, der auf der Schaltfläche angezeigt wird, mit der Benutzer den Zweitfaktor der Authentifizierung bestätigen.
  - e) Geben Sie im Feld **Schaltflächentext verwerfen** den Text ein, der auf der Schaltfläche angezeigt wird, mit der Benutzer den Zweitfaktor der Authentifizierung verwerfen.
  - f) Geben Sie im Feld **Timeout (Sekunden)** die Zeitdauer in Sekunden bis zum Ablauf der Authentifizierungstransaktion an.
8. Klicken Sie auf **Hinzufügen**.
9. Wiederholen Sie diese Schritte für jedes VPN-Gateway, das Sie hinzufügen möchten.
10. Klicken Sie auf **Speichern**.

## Aktualisieren einer Verbindung zu einem VPN-Gateway

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry 2FA-Server**.
2. Klicken Sie auf den Namen des 2FA-Servers, den Sie konfigurieren möchten.
3. Klicken Sie auf den Namen des VPN-Servers, den Sie aktualisieren möchten.
4. Aktualisieren Sie wie gewünscht die Konfiguration. Weitere Informationen finden Sie in den Schritten 4 bis 7 unter [Konfigurieren des BlackBerry 2FA-Servers für die Verbindung mit einem VPN-Gateway](#).
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern**.

## Löschen einer Verbindung zu einem VPN-Gateway

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry 2FA-Server**.
2. Klicken Sie neben dem VPN-Server, den Sie löschen möchten, auf .
3. Klicken Sie auf **Ja**.
4. Klicken Sie auf **Speichern**.

# Konfigurieren der Verbindung zum REST-API-Endpunkt

Der REST-API-Endpunkt des BlackBerry 2FA-Servers wird über ein vom Server authentifiziertes HTTPS geschützt. Sie müssen Ihre benutzerdefinierten Dienste so konfigurieren, dass sie den BlackBerry 2FA-Server als vertrauenswürdig behandeln. Sie haben die Wahl aus folgenden Optionen:

- Sie können das selbst signierte Standardzertifikat verwenden, das bei der Installation des BlackBerry 2FA-Servers generiert wird. Das selbst signierte Standardzertifikat befindet sich in der Datei `bb2fa-config/restkeystore.jks`. Ihre Client-Anwendung muss so konfiguriert sein, dass sie dieses Zertifikat explizit als vertrauenswürdig behandeln. Der Standardserverport lautet 5443.
- Sie können Ihr eigenes, von einer Zertifizierungsstelle signiertes Zertifikat bereitstellen, indem Sie es in einer Java-Keystore-Datei unter dem Alias „bb2fa“ importieren (als Schlüsselalgorithmus wird RSA 2048 empfohlen). Kopieren Sie die Keystore-Datei in das Verzeichnis `bb2fa-config`, und aktualisieren Sie den Keystore-Dateinamen und das Kennwort auf der Konfigurationsseite des BlackBerry 2FA-Servers in BlackBerry UEM.

Die benutzerdefinierten Dienste werden auf jeden Fall über die HTTP-Standardauthentifizierung (Benutzername und Kennwort) authentifiziert, die in der Anforderung als Kopfzeilen gesendet werden.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry 2FA-Server**.
2. Klicken Sie auf den Namen des 2FA-Servers, den Sie konfigurieren möchten.
3. Geben Sie im Abschnitt **REST-Schnittstellenkonfiguration** die erforderlichen Informationen ein.
4. Klicken Sie auf **Speichern**.

## Konfigurieren der REST-API-Endpunktkonnektivität

Um die Konnektivität zwischen Client-Apps und dem REST-API-Endpunkt des BlackBerry 2FA-Servers zu konfigurieren, müssen Sie Ihre Client-Anwendungen so konfigurieren, dass sie den BlackBerry 2FA-Server als vertrauenswürdig behandeln.

Die Client-Apps werden über die HTTP-Standardauthentifizierung (Benutzername und Kennwort) authentifiziert, die in der Anforderung als Kopfzeilen gesendet werden. Der REST-API-Endpunkt wird durch eine vom Server authentifizierte HTTPS geschützt (`https://<Hostname>:<Port>/<Präfix>/`). Der Standardport lautet 5443, das Standardpräfix „rest“. Auf dem Endpunkt werden folgende REST-Anforderungen unterstützt:

Pfad	Typ	Beschreibung	Notizen
<code>/&lt;Präfix&gt;/twofactor</code>	POST	Zwei-Faktor-Authentifizierungsanforderung	

Die Anforderungsnachricht wird per HTTP POST gesendet und als JSON formatiert. Sie enthält folgende Parameter:

Parameter	Typ	Beschreibung	Notizen
username	Zeichenfolge	Benutzername	
-Kennwort	Zeichenfolge	Benutzerkennwort, oder Einmalkennwort und Benutzerkennwort	Optional, abhängig von der Richtlinie

Parameter	Typ	Beschreibung	Notizen
policy	Ganze Zahl	Authentifizierungsoption: <ul style="list-style-type: none"> <li>• 0: Ein-Faktor-Authentifizierung mittels Unternehmenskennwort</li> <li>• 1: Zwei-Faktor-Authentifizierung mittels Unternehmenskennwort</li> <li>• 2: Zwei-Faktor-Authentifizierung mit passivem Gerätekenwort</li> <li>• 3: Zwei-Faktor-Authentifizierung mit aktivem Gerätekenwort</li> </ul>	
oneTimePassword	Zeichenfolge	Einmalkennwort	Optional
messageTitle	Zeichenfolge	Dialog „Titeltext“	Optional
message	Zeichenfolge	Dialog „Nachrichtentext“	Optional
confirmButtonText	Zeichenfolge	Dialog „Schaltflächentext bestätigen“	Optional
declineButtonText	Zeichenfolge	Dialog „Schaltflächentext verwerfen“	Optional
timeout	Ganze Zahl	Dialog „Timeout (Sekunden)“	Optional

Der Text der Antwortnachricht wird als JSON mit folgenden Parametern formatiert:

Parameter	Typ	Beschreibung	Notizen
info	Zeichenfolge	Informationsnachricht	

Die Antwortnachricht enthält außerdem folgende HTTP-Statuscodes:

Status	Beschreibung	Notizen
200	OK	Authentifizierung erfolgreich
400	Ungültige Anforderung	Ungültige Parameter
401	Nicht autorisiert	Authentifizierung fehlgeschlagen
403	Abgelehnt	Vom Benutzer abgelehnte Authentifizierung
500	Interner Serverfehler	Interner Fehler

# Erstellen eines REST-API-Client im BlackBerry 2FA-Server

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskontrolle auf **Einstellungen > Externe Integration > BlackBerry 2FA-Server**.
2. Klicken Sie auf den Namen des 2FA-Servers, den Sie konfigurieren möchten.
3. Klicken Sie im Abschnitt **REST-Clientkonfiguration** auf **+**.
4. Geben Sie im Feld **REST-Clientname** einen Anzeigenamen für den Client ein.
5. Geben Sie im Feld **REST-Client-ID** einen Namen für den Client ein, der mit dem Kennwort verknüpft ist.
6. Geben Sie im Feld **Kennwort** ein Kennwort ein. Das Kennwort muss aus mindestens acht Zeichen bestehen.
7. Geben Sie im Feld **Kennwort bestätigen** erneut das Kennwort ein.
8. Klicken Sie auf **Hinzufügen**.
9. Wiederholen Sie diese Schritte für jeden Client, den Sie hinzufügen möchten.
10. Klicken Sie auf **Speichern**.

# Aktivieren der MS-CHAP-Authentifizierung für Benutzer in einer Domäne

Sie können einen BlackBerry 2FA-Server aktivieren, damit er die MS-CHAPv1- und MS-CHAPv2-Authentifizierung für RADIUS-Anforderungen (z. B. für Anforderungen, die von einem VPN-Gateway kommen) für Benutzer unterstützt, die Mitglied der ausgewählten Domäne sind. Die Domäne ist für diese Option verfügbar, da der 2FA-Server auf einem Host ausgeführt wird, der mit einer Active Directory-Domäne verbunden ist, mit der auch BlackBerry UEM verbunden ist.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry 2FA-Server**.
2. Klicken Sie auf den Namen des 2FA-Servers, den Sie konfigurieren möchten.
3. Wählen Sie im Abschnitt **Active Directory-Konfiguration** die Domäne aus, für die Sie die MS-CHAP-Authentifizierung aktivieren möchten. Um die MS-CHAP-Authentifizierung zu deaktivieren, entfernen Sie die Auswahl für diese Domäne.
4. Klicken Sie auf **Speichern**.



# Konfigurieren der BlackBerry 2FA-App

Sie können die Standardmeldung anpassen, die BlackBerry 2FA Benutzern anzeigt, wenn sich diese an Ihren Ressourcen anmelden. Außerdem können Sie die Zeitdauer in Sekunden bis zum Ablauf der Authentifizierungsaufforderung festlegen.

Sie können diese Einstellungen für jedes VPN-Gateway, das Sie konfigurieren, überschreiben. Weitere Informationen zur Konfiguration von VPN-Gateways finden Sie unter [Konfigurieren des BlackBerry 2FA-Servers für die Verbindung mit einem VPN-Gateway](#).

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry 2FA-Server**.
2. Klicken Sie auf den Namen des 2FA-Servers, den Sie konfigurieren möchten.
3. Nehmen Sie im Abschnitt **Standardgeräteaufforderung** folgende Einstellungen vor:
  - a) Geben Sie im Feld **Titel** den Titel an, der in der Nachricht der App angezeigt werden soll. Beispielsweise „VPN des Beispielunternehmens“.
  - b) Geben Sie im Feld **Nachricht** die Nachricht ein, die die App Benutzern anzeigen soll. In dieser Nachricht wird Benutzern erklärt, was von ihnen benötigt wird.
  - c) Geben Sie im Feld **Schaltflächentext bestätigen** den Text ein, der auf der Schaltfläche angezeigt wird, mit der Benutzer den Zweitfaktor der Authentifizierung bestätigen.
  - d) Geben Sie im Feld **Schaltflächentext verwerfen** den Text ein, der auf der Schaltfläche angezeigt wird, mit der Benutzer den Zweitfaktor der Authentifizierung verwerfen.
  - e) Geben Sie im Feld **Timeout (Sekunden)** die Zeitdauer in Sekunden bis zum Ablauf der Authentifizierungstransaktion an.
4. Klicken Sie auf **Speichern**.

# Zuordnen eines VPN-Gateways oder einer REST-Client-Konfiguration zu einer Benutzergruppe

Um Benutzer für die Verwendung von VPN- oder REST-Clients zu autorisieren, müssen Sie ein VPN-Gateway oder eine REST-Client-Konfiguration zu Benutzergruppen zuordnen. Sie können Benutzergruppen erstellen, die die Benutzer beinhalten, denen Sie die Konfigurationen zuweisen möchten. Benutzer können nur die Konfigurationen verwenden, die ihnen zugewiesen sind.

**Bevor Sie beginnen:** Führen Sie einen der folgenden Schritte aus:

- [Konfigurieren des BlackBerry 2FA-Servers für die Verbindung mit einem VPN-Gateway](#)
  - [Erstellen eines REST-API-Client im BlackBerry 2FA-Server](#)
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, der Sie eine Konfiguration zuordnen möchten.
  3. Klicken Sie auf die Registerkarte **BlackBerry 2FA**.
  4. Klicken Sie auf **+**.
  5. Wählen Sie aus der Dropdown-Liste eine Geräte-Client-Konfiguration aus.
  6. Klicken Sie auf **Zuweisen**.

# Installieren der BlackBerry 2FA-App auf Geräten

BlackBerry 2FA ist für iOS-, Android- und BlackBerry 10-Geräte verfügbar.

## iOS- und Android-Geräte

Bei Verwendung von iOS- und Android-Geräten sind BlackBerry 2FA-Funktionen in der BlackBerry UEM Client-App enthalten. Benutzer müssen den BlackBerry UEM Client herunterladen, um ihr Gerät für BlackBerry UEM zu aktivieren und 2FA zu nutzen.

Benutzer können die BlackBerry UEM Client-App aus dem Google Play und dem App Store herunterladen.

## BlackBerry 10-Geräte

Bei BlackBerry 10-Geräten müssen Sie die BlackBerry 2FA-App mithilfe von BlackBerry UEM an die Geräte senden. Führen Sie folgende Aktionen mithilfe von BlackBerry UEM aus:

- Verwenden Sie ggf. die BlackBerry UEM-Verwaltungskonsole, um einen freigegebenen Netzwerkpfad für interne Apps anzugeben.
- Fügen Sie in der BlackBerry UEM-Verwaltungskonsole die BlackBerry 2FA-Appdatei (.bar) als interne App hinzu. Die BlackBerry 2FA-App befindet sich hier: <https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B>
- Weisen Sie die App in der BlackBerry UEM-Verwaltungskonsole zu Benutzerkonten oder Gruppen zu.

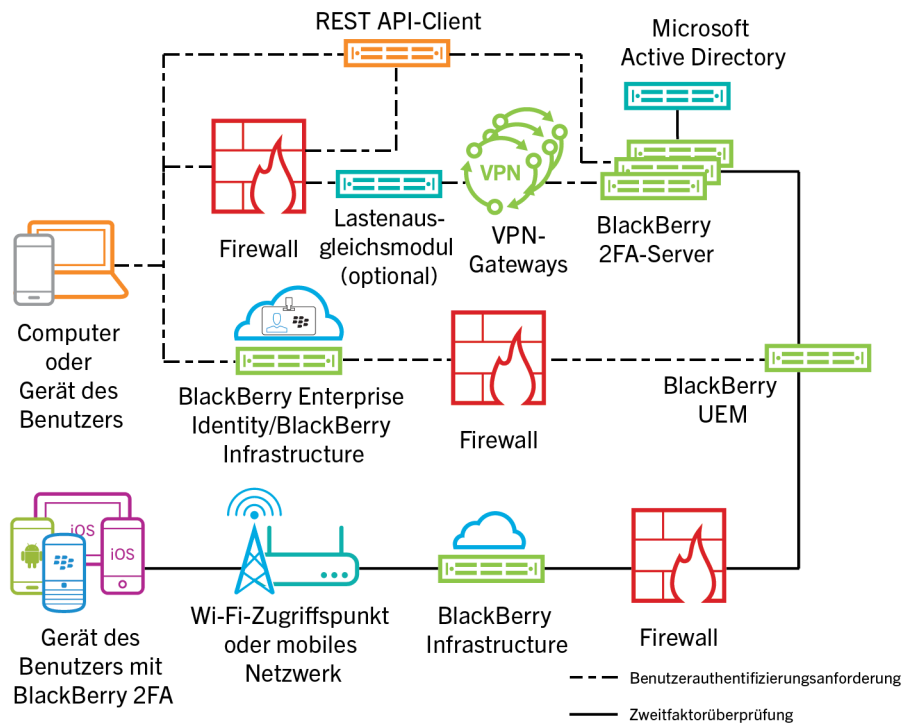
Bei Geräten mit einem geschäftlichen Bereich wird die App dort installiert. Benutzer können sie auch mithilfe von BlackBerry World für geschäftliche Zwecke installieren, wenn Sie die Installation nicht als obligatorisch festlegen.

Weitere Informationen über das Senden von Apps finden Sie in der [BlackBerry UEM-Dokumentation zur Administration](#).

# Architektur: Hohe Verfügbarkeit für BlackBerry 2FA

BlackBerry 2FA unterstützt Aktiv-Aktiv-Hochverfügbarkeit. Sie können mehrere Instanzen des BlackBerry 2FA-Servers für die Lastverteilung bei Authentifizierungsanforderungen und zur Erhöhung der Zuverlässigkeit installieren.

Im folgenden Diagramm ist ein Szenario zur Hochverfügbarkeit dargestellt. VPN-Lösungen können ein Lastenausgleichsmodul umfassen, und in diesem Szenario ist keine separate Lastverteilung erforderlich.



## Konfigurieren des BlackBerry 2FA-Servers für hohe Verfügbarkeit

Sie können hierfür dieselben Ports wie für alle BlackBerry 2FA-Server verwenden.

Um eine eindeutige Verschlüsselung von Konfigurationsdaten zu bearbeiten, wird empfohlen, dass Sie die Datei `bb2fa-config.json` nicht zwischen BlackBerry 2FA-Servern kopieren. Sie müssen jeden Server separat in der BlackBerry UEM-Verwaltungskonsole konfigurieren.

Aufgabe	Beschreibung
1	Richten Sie für Ihr VPN-Gateway hohe Verfügbarkeit ein, sofern Sie dies noch nicht getan haben. Weitere Informationen finden Sie in der Dokumentation zu Ihrem VPN-Gateway.

Aufgabe	Beschreibung
2	Installieren Sie mindestens zwei BlackBerry 2FA-Server. Generieren Sie für jeden Server eine Aktivierungsdatei und laden Sie diese herunter. Bei aufeinanderfolgenden Installationen haben Sie die Wahl, ob Sie die BlackBerry 2FA-Appdateien auswählen. Sie müssen die Dateien nur einmal installieren. Weitere Informationen finden Sie in der <a href="#">Dokumentation zu Installation und Upgrade von BlackBerry 2FA-Servern</a> .
3	Erstellen Sie ein Profil für die BlackBerry 2FA-Server auf dem VPN-Server. Weitere Informationen finden Sie unter <a href="#">Konfigurieren einer Verbindung zwischen dem BlackBerry 2FA-Server und einem VPN-Gateway</a> .
4	Verbinden Sie die einzelnen BlackBerry 2FA-Server mit einem VPN-Gateway. Weitere Informationen finden Sie unter <a href="#">Konfigurieren des BlackBerry 2FA-Servers für die Verbindung mit einem VPN-Gateway</a> .
5	Konfigurieren der Verbindung zum REST-API-Endpunkt
6	Erstellen eines REST-API-Client im BlackBerry 2FA-Server.
7	Aktivieren der MS-CHAP-Authentifizierung für Benutzer in einer Domäne
8	Konfigurieren der BlackBerry 2FA-App
9	Zuordnen eines VPN-Gateways oder einer REST-Client-Konfiguration zu einer Benutzergruppe
10	Senden Sie die BlackBerry 2FA-App bei Bedarf an die entsprechenden Geräte. Weitere Informationen finden Sie unter <a href="#">Installieren der BlackBerry 2FA-App auf Geräten</a> .
11	
12	

# Protokollierung und Reporting

Das BlackBerry 2FA speichert seine Protokolldateien unter `<install_dir>\logs`. Es gibt vier Protokolldateien:

- Das `bb2fa.log` ist die Hauptprotokolldatei, die alle Meldungen des BlackBerry 2FA-Servers enthält. Sie beinhaltet beispielsweise Meldungen zum Startvorgang und zum Herunterfahren sowie Meldungen zum Authentifizierungsfortschritt.
- Die Datei `key_log.txt` enthält Meldungen mit Bezug zu Erstellung und Status der Schlüssel, die der BlackBerry 2FA-Server für den Schutz vertraulicher Informationen, etwa Kennwörtern, benötigt.
- Die Datei `bb2fa-audit.log` enthält durch Komma getrennte Überwachungsdaten. Darin werden alle Authentifizierungsanforderungen aufgezeichnet, die der BlackBerry 2FA-Server vorgenommen hat.
- Die Datei `winrun_log.txt` enthält Meldungen zum Startvorgang und der Ausführung des BlackBerry 2FA-Servers, wenn Sie diesen in den Windows-Diensten ausführen.

BlackBerry 2FA verwendet zur Protokollierung das Apache log4j-Protokollierungstool. Standardmäßig schreibt der BlackBerry 2FA-Server Protokollmeldungen auf Informationsebene.

Der BlackBerry 2FA-Server erzeugt täglich neue Protokoll- und Überwachungsdateien. Wenn die Protokoll- oder Überwachungsdatei erstellt wird, erhält die vorherige Protokoll- oder Überwachungsdatei den Zeitstempel `bb2fa.<Datum>.log` oder `b2fa-audit.log.<Datum>`.

Sie können die Protokollierungsebene und den Ort, an dem BlackBerry 2FA die Protokoll- und Überwachungsdateien speichert, unter Verwendung der Datei `log4j.properties` in `<install_dir>\bb2fa-config` ändern. Weitere Informationen finden Sie unter <http://logging.apache.org/log4j/2.x/> im *Benutzerhandbuch für Apache log4j 2*.

## Überwachung von Authentifizierungsanforderungen

### BlackBerry 2FA-Server

Der BlackBerry 2FA-Server zeichnet jede von ihm erstellte Authentifizierungsanforderung in einer Überwachungsprotokolldatei auf, wenn die Anforderung abläuft. Die Überwachungsprotokolldatei enthält die folgenden Informationen zu jeder Anforderung:

- Datum
- Uhrzeit
- Transaktion-ID
- Client-Name
- Client-IP-Adresse
- Benutzername
- Authentifizierungsoption
- dem Benutzer zugewiesene BlackBerry 10-Geräte
- dem Benutzer zugewiesene Drittanbietergeräte
- dem Benutzer zugewiesene BlackBerry OS-Geräte
- Gerät, das auf die Authentifizierungsanforderung geantwortet hat
- Zeit (in Sekunden), die für den Abschluss der Authentifizierungsanforderung benötigt wurde
- Ergebnis der Anforderung

Beispiel:

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

Die Überwachungsprotokolldatei enthält durch Komma getrennte Werte, und Sie können diese mit jeder Software öffnen, die CSVs unterstützt. Sie wird als `bb2fa-audit.log` bezeichnet und unter `<install_dir>\logs` gespeichert.

### BlackBerry UEM

Weitere Informationen über die BlackBerry UEM-Protokollierung finden Sie in der [BlackBerry UEM-Dokumentation zur Administration](#).

## Zentralisieren von Protokollierungs- oder Überwachungsvorgängen mit Syslog

Sie können den BlackBerry 2FA-Server so konfigurieren, dass er Protokolldateien, Überwachungsdateien oder beides auf einen zentralen Syslog-Server anstatt in lokale Dateien schreibt.

**Hinweis:** Diese Aufgabe zeigt eine Möglichkeit, die Protokollierung zu zentralisieren. Weitere Informationen zum Konfigurieren der Protokollierung finden Sie unter <http://logging.apache.org/log4j/2.x/> im *Benutzerhandbuch für Apache log4j 2*.

1. Navigieren Sie zum Ordner `<install_dir>\bb2fa-config`.
2. Navigieren Sie zum Ordner `<install_dir>/bb2fa-config`.
3. Sichern Sie die Datei `log4j.properties`.
4. Öffnen Sie die Datei `log4j.properties` in einem Texteditor.
5. Um Protokollmeldungen an einen zentralen Syslog-Server zu senden, gehen Sie wie folgt vor:
  - a) Ändern Sie den Wert von `log4j.rootLogger` auf einen der folgenden Werte:
    - Um Protokollmeldungen nur auf einen Syslog-Server zu schreiben: `ALL, syslog`
    - Um Protokollmeldungen lokal und auf einen Syslog-Server zu schreiben: `ALL, logfile, syslog`
  - b) Fügen Sie die folgenden Zeilen hinzu:

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

- c) Legen Sie für den Wert `log4j.appender.syslog.syslogHost` den Hostnamen und Port Ihres Syslog-Servers fest.
- d) Um die lokale Protokollierung zu entfernen, löschen Sie optional die folgenden Zeilen:

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

6. Um Überwachungsmeldungen an einen zentralen Syslog-Server zu senden, gehen Sie wie folgt vor:

a) Ändern Sie den Wert von `log4j.logger.auditLogger` auf einen der folgenden Werte:

- Um Überwachungsmeldungen nur auf einen Syslog-Server zu schreiben: `ALL, auditsyslog`
- Um Überwachungsmeldungen lokal und auf einen Syslog-Server zu schreiben: `ALL, auditfile, auditsyslog`

b) Fügen Sie die folgenden Zeilen hinzu:

```
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
log4j.appender.auditsyslog.syslogHost=<Hostname>:<Port>
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

c) Legen Sie für den Wert `log4j.appender.syslog.syslogHost` den Hostnamen und Port Ihres Syslog-Servers fest. Für die Überwachungsdatei und die Protokolldatei müssen Sie unterschiedliche Ports verwenden.

d) Um die lokale Überwachung zu entfernen, löschen Sie optional die folgenden Zeilen:

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

7. Speichern Sie die Änderungen.

8. Starten Sie den in den Windows-Diensten aufgeführten BlackBerry 2FA-Dienst neu.

9. Starten Sie den BlackBerry 2FA-Dienst neu.

### Beispieldatei `log4j.properties` mit Syslog- und lokaler Protokollierung

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

log4j.logger.auditLogger=ALL, auditfile, auditsyslog

# Wir möchten die Ausgabe von Apache CFX und Jetty steuern,
# die auf Fehlerbehebungsebene sehr ausführlich sind.
log4j.logger.org.apache.cxf=INFO
log4j.logger.org.eclipse.jetty=INFO

# Umleitung der Protokolle in eine lokale Protokolldatei
log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
log4j.appender.logfile.layout.ConversionPattern=%d{ISO8601}[%-5p] (%t) %c - %m%n
log4j.appender.logfile.datePattern='.'yyyy-MM-dd
log4j.appender.logfile.Threshold = INFO
log4j.appender.logfile.append=true
log4j.appender.logfile.File=logs/bb2fa.log

# Umleitung der Protokolle zu einem Remote-Syslog-Server
log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.syslog.Threshold = INFO
```



```
log4j.appender.syslog.syslogHost=syslog.example.com:514
log4j.appender.syslog.layout=org.apache.log4j.PatternLayout
log4j.appender.syslog.layout.ConversionPattern=[%-5p] %c - %m%n

# Umleitung der Überwachungsmeldungen in eine lokale Überwachungsdatei
log4j.appender.auditfile=org.apache.log4j.DailyRollingFileAppender
log4j.appender.auditfile.layout=org.apache.log4j.PatternLayout
log4j.appender.auditfile.layout.ConversionPattern=%d{yyyy-MM-dd},%d{HH:mm:ss.SSS},
%m%n
log4j.appender.auditfile.datePattern='.'yyyy-MM-dd
log4j.appender.auditfile.Threshold = INFO
log4j.appender.auditfile.append=true
log4j.appender.auditfile.File=logs/bb2fa-audit.log

# Umleitung der Überwachungsmeldungen zu einem Remote-Syslog-Server
# (Sie benötigen einen anderen Port zum Generieren einer anderen Datei.)
log4j.appender.auditsyslog=org.apache.log4j.net.SyslogAppender
log4j.appender.auditsyslog.Threshold = INFO
log4j.appender.auditsyslog.syslogHost=syslog.example.com:515
log4j.appender.auditsyslog.layout=org.apache.log4j.PatternLayout
log4j.appender.auditsyslog.layout.ConversionPattern=%d{yyyy-MM-dd},
%d{HH:mm:ss.SSS},%m%n
```

# Authentifizierungsoptionen

BlackBerry 2FA bietet folgende Authentifizierungsoptionen:

**Hinweis:** Wenn einem Benutzer eine Zwei-Faktor-Option zugewiesen ist, ist automatisch die Verwendung eines OTP-Token zulässig, wenn ihm dies zugewiesen ist.

Authentifizierungsoption	Beschreibung	Nützlich, wenn
Zwei-Faktor-Authentifizierung mittels Unternehmenskennwort	<p>Wenn sich ein Benutzer anmeldet, gibt er einen Benutzernamen und ein Verzeichniskennwort ein und erhält daraufhin eine Eingabeaufforderung zum Bestätigen der Authentifizierungsanforderung auf dem Gerät.</p> <p>Wenn einem Benutzer diese Option zugewiesen ist, darf er automatisch ein OTP-Token verwenden, wenn ihm eines zugewiesen ist.</p> <p>Diese Option wird auf allen Geräten unterstützt.</p>	Für Ihr Unternehmen ist Sicherheit das wichtigste Ziel bei jeder Bereitstellung.
Zwei-Faktor-Authentifizierung mit passivem Gerätekenwort	<p>Wenn sich ein Benutzer anmeldet, gibt er nur einen Benutzernamen an und erhält dann eine Aufforderung, die Authentifizierungsanforderung zu bestätigen. Wenn das Gerät gesperrt ist, muss der Benutzer das Gerätekenwort eingeben, bevor er die Eingabeaufforderung bestätigen kann.</p> <p>Wenn einem Benutzer diese Option zugewiesen ist, darf er automatisch ein OTP-Token verwenden, wenn ihm eines zugewiesen ist.</p> <p>Bei BlackBerry 10-Geräten müssen Benutzer das Kennwort für den geschäftlichen Bereich eingeben, wenn der geschäftliche Bereich gesperrt ist.</p> <p>Diese Option wird auf allen Geräten unterstützt.</p>	Für Ihr Unternehmen ist Benutzerfreundlichkeit das wichtigste Ziel bei jeder Bereitstellung.

Authentifizierungsoption	Beschreibung	Nützlich, wenn
Zwei-Faktor-Authentifizierung mit aktivem Gerätekennwort	<p>Wenn sich ein Benutzer anmeldet, gibt er nur einen Benutzernamen an und erhält dann eine Aufforderung, die Authentifizierungsanforderung auf seinem Gerät zu bestätigen. Der Benutzer muss das Gerätekennwort immer eingeben, bevor er die Eingabeaufforderung bestätigen kann.</p> <p>Wenn einem Benutzer diese Option zugewiesen ist, darf er automatisch ein OTP-Token verwenden, wenn ihm eines zugewiesen ist.</p> <p>Bei BlackBerry 10-Geräten müssen Benutzer das Kennwort für den geschäftlichen Bereich eingeben.</p> <p>Diese Option wird für BlackBerry 10- und BlackBerry-Geräte mit den Betriebssystemversionen 6.0 bis 7.1 unterstützt.</p>	Ihr Unternehmen legt Wert auf Benutzerfreundlichkeit, möchte sich jedoch davor schützen, dass jemand ein nicht gesperrtes Gerät hernimmt und die Geräteaufforderung akzeptiert.
Ein-Faktor-Authentifizierung mittels Unternehmenskennwort	Benutzer melden sich nur mit der Microsoft Active Directory-Authentifizierung an.	<ul style="list-style-type: none"> <li>• Der Benutzer hat kein Gerät.</li> <li>• Der Benutzer hat sein Gerät vergessen oder verloren.</li> <li>• Der Benutzer muss keinen zweiten Faktor der Authentifizierung verwenden.</li> </ul>

**Hinweis:** In BlackBerry 2FA-Version 2.5 können Sie Benutzerauthentifizierungsoptionen auf sieben verschiedene Weisen konfigurieren. Standardmäßig werden die Authentifizierungsoptionen mithilfe eines BlackBerry 2FA-Profiles in BlackBerry UEM konfiguriert. Sie können diese Standardkonfiguration für Authentifizierungsanforderungen, die über die REST API oder über VPN-Gateways und andere RADIUS-Clients gesendet werden, allerdings überschreiben. Weitere Informationen finden Sie unter [Konfigurieren der REST-API-Endpunktconnectivität](#) oder [Konfigurieren einer Verbindung zwischen dem BlackBerry 2FA-Server und einem VPN-Gateway](#).

# Benutzernamen, Kennwörter und Verzeichnisse

BlackBerry 2FA authentifiziert Benutzer, die in einem Verzeichnis verfügbar sind. Sowohl der BlackBerry 2FA-Server als auch BlackBerry UEM sind mit diesen Verzeichnissen verbunden. Basierend darauf, wie diese Verbindungen konfiguriert sind, unterstützt BlackBerry 2FA vier Benutzertypen:

- Benutzer in einer Microsoft Active Directory-Domäne, die sowohl mit einem BlackBerry 2FA-Server als auch mit BlackBerry UEM verbunden ist
- Benutzer in einer Microsoft Active Directory-Domäne, die nicht mit einem BlackBerry 2FA-Server aber mit BlackBerry UEM verbunden ist
- Benutzer in einem LDAP-Verzeichnis, das mit BlackBerry UEM verbunden ist
- Benutzer in einem lokalen BlackBerry UEM-Verzeichnis

Wenn sich ein Benutzer anmeldet, muss er einen Benutzernamen und optional ein Kennwort angeben.

## Benutzername

Der Benutzername muss einer eindeutigen Benutzereingabe in einem Verzeichnis entsprechen. Kann der Benutzer nicht eindeutig aufgelöst werden, schlägt die Authentifizierungsanforderung fehl. Zur Angabe des Verzeichnisses, in dem sich der Benutzer befindet, muss der Benutzer nach folgenden Benutzernamen für jeden Benutzertyp identifiziert werden:

- Die folgenden Benutzernamen werden für Benutzer in einer Microsoft Active Directory-Domäne unterstützt, die sowohl mit einem BlackBerry 2FA-Server als auch mit BlackBerry UEM verbunden ist. Diese Benutzer können sich mit PAP, MSCHAPv1, MSCHAPv2 und EAP-MSCHAPv2 authentifizieren und so konfiguriert werden, dass sie für jeden REST-API-Client Autorisierungsgruppen verwenden und Authentifizierungs-Überschreibungsgruppen für alle VPN-Gateways.  
<Benutzername> (z. B. jschmitt)  
<Benutzername>@<NetBIOS-Domänenname> (z. B. jschmitt@unternehmen)  
<NetBIOS-Domänenname>\<Benutzername> (z. B. Unternehmen\jschmitt)  
<E-Mail-Adresse> (z. B. jschmitt@unternehmen.com)
- Die folgenden Benutzernamen werden für Benutzer in einer Microsoft Active Directory-Domäne unterstützt, die nicht mit einem BlackBerry 2FA-Server, aber mit BlackBerry UEM verbunden ist. Diese Benutzer können sich nur mit dem PAP authentifizieren.  
<Benutzername> (z. B. jschmitt)  
<Benutzername>@<NetBIOS-Domänenname> (z. B. jschmitt@unternehmen)  
<NetBIOS-Domänenname>\<Benutzername> (z. B. Unternehmen\jschmitt)  
<E-Mail-Adresse> (z. B. jschmitt@unternehmen.com)
- Die folgenden Benutzernamen werden für Benutzer in einem LDAP-Verzeichnis unterstützt, das mit einem BlackBerry UEM-Server verbunden ist. Diese Benutzer müssen sich mit dem PAP authentifizieren.

**Hinweis:** Der BlackBerry 2FA-Server kann keine Verbindung zu diesem Verzeichnis herstellen.

<Benutzername> (z. B. jschmitt)  
<Benutzername>@<Verzeichnis FQDN> (z. B. jschmitt@unternehmen.ldap.net)  
<Verzeichnis FQDN>\<Benutzername> (z. B. Unternehmen.ldap.net\jschmitt)  
<E-Mail-Adresse> (z. B. jschmitt@unternehmen.com)

- Die folgenden Benutzernamen werden für Benutzer in einem lokalen BlackBerry UEM-Verzeichnis unterstützt. Diese Benutzer müssen sich mit dem PAP authentifizieren.

**Hinweis:** Der BlackBerry 2FA-Server kann keine Verbindung zu diesem Verzeichnis herstellen.

<Benutzername> (z. B. jschmitt)

<Benutzername>@lokal (z. B. jschmitt@lokal)  
lokal\<Benutzername> (z. B. lokal\jschmitt)  
<E-Mail-Adresse> (z. B. jschmitt@unternehmen.com)

### **Kennwort**

Abhängig von der Authentifizierungsoption, die für Benutzer konfiguriert wurde, müssen diese bei der Anmeldung ein Verzeichniskennwort eingeben.

Wenn sich ein Benutzer mit einem Einmalkennwort (One-Time Password, OTP)-Token authentifiziert, muss er das OTP und das Verzeichniskennwort eingeben, unabhängig von der Option für die Zwei-Faktor-Authentifizierung, die für ihn konfiguriert wurde.

- Zur Anmeldung an einem VPN muss der Benutzer sowohl das OTP- als auch das Verzeichniskennwort im Kennwortfeld eingeben. Zuerst wird das OTP eingegeben, anschließend das Verzeichniskennwort, und es dürfen keine Leerzeichen oder Trennzeichen hinzugefügt werden.
- Bei Anmeldung über einen Client, der mit einer REST-API verbunden ist, muss der Benutzer das Verzeichniskennwort in das Kennwortfeld eingeben und anschließend das OTP in das dafür vorgesehene Feld.

# REST-API-Endpunkt

Der BlackBerry 2FA-Server hat einen externen REST-API-Endpunkt, der BlackBerry 2FA für benutzerdefinierte Dienste, wie Webanwendungen und SIP-Client-Anwendungen erweitert. Sie können die BlackBerry 2FA-Serverkonfigurationsseite in der BlackBerry UEM-Verwaltungskonsolle verwenden, um einen REST-Client zu erstellen. Weitere Informationen finden Sie unter [Konfigurieren der REST-API-Endpunktkonnektivität](#).

# VPN-Gateways

Sie können die BlackBerry 2FA-Serverkonfigurationsseite in der BlackBerry UEM-Verwaltungskonsole verwenden, um eine Verbindung zu einem VPN-Gateway zu erstellen. Die Verbindung zwischen einem VPN-Gateway und dem BlackBerry 2FA-Server wird mit RADIUS hergestellt. Weitere Informationen finden Sie unter [Konfigurieren einer Verbindung zwischen dem BlackBerry 2FA-Server und einem VPN-Gateway](#).

# Glossar

<b>API</b>	Programmierschnittstelle
<b>Zertifizierungsstelle</b>	Zertifizierungsstelle
<b>DNS</b>	Domain Name System
<b>ECDH</b>	Elliptic Curve Diffie-Hellman
<b>EAP</b>	Extensible Authentication Protocol (erweiterbares Authentifizierungsprotokoll)
<b>EMM</b>	Enterprise Mobility Management
<b>FQDN</b>	Fully Qualified Domain Name
<b>HTTP</b>	Hypertext Transfer Protocol (Hypertextübertragungsprotokoll)
<b>HTTPS</b>	Hypertext Transfer Protocol over Secure Sockets Layer
<b>IP</b>	Internet Protocol
<b>IT-Richtlinie</b>	Eine IT-Richtlinie besteht aus verschiedenen Regeln, die die Sicherheitsmerkmale und das Verhalten von Geräten steuern.
<b>IKE</b>	Internet Key Exchange
<b>MAM</b>	Mobile Application Management
<b>MDM</b>	Mobile Geräteverwaltung (Mobile Device Management)
<b>MS-CHAP</b>	Microsoft Challenge Handshake Authentication Protocol (Authentifizierungsprotokoll von Microsoft)
<b>NAS</b>	Network-Attached Storage
<b>NTLM</b>	NT LAN Manager (Authentifizierungsverfahren für Rechnernetze)
<b>OTP</b>	Einmalkennwort (One-Time Password)
<b>PAP</b>	Push Access Protocol
<b>RADIUS</b>	Remote Authentication Dial-In User Service
<b>REST</b>	Representational State Transfer



<b>SAML</b>	Security Assertion Markup Language (Auszeichnungssprache für Sicherheitsbestätigungen)
<b>SIP</b>	Session Initiation Protocol (Netzprotokoll zum Aufbau einer Kommunikationsverbindung)
<b>SSL</b>	Secure Sockets Layer
<b>TLS</b>	Transport Layer Security
<b>UEM</b>	Unified Endpoint Manager
<b>VPN</b>	Virtual Private Network

# Rechtliche Hinweise

©2018 BlackBerry Limited. Sämtliche 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 weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

Android und G Suites sind Marken von Google, Inc. Apache log4j ist eine Marke von The Apache Software Foundation. Barracuda ist eine Marke von Barracuda Networks, Inc. Box ist eine Marke, Dienstleistungsmarke oder eingetragene Marke von Box, Inc. Cisco und Cisco AnyConnect sind Marken von Cisco Systems, Inc. und/oder seiner angegliederten Unternehmen in den USA und einigen anderen Ländern. Citrix und NetScaler sind Marken von Citrix Systems, Inc. und/oder einer oder mehrerer Tochtergesellschaften, die beim United States Patent and Trademark Office und in anderen Ländern eingetragen sein können. F5 und BIG-IP iOS 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. Java und JavaScript sind Marken von Oracle und/oder deren Tochterunternehmen. Microsoft, Active Directory, Internet Explorer, SQL Server, Windows und Windows Phone sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Salesforce ist eine Marke von salesforce.com, inc. und wird hier mit entsprechender Genehmigung verwendet. 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, Angemessenheit, 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, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDE QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, CHANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDE LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTPRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE GELTEN FÜR 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 JEDLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEDLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE, VERSCHÄRFTE SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIRECTE, 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 ANGEHÖRENDE 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 Diensteanbieter 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  
200 Bath Road  
Slough, Berkshire SL1 3XE  
Großbritannien

Veröffentlicht in Kanada