



BlackBerry 2FA

Administratorhandbuch

Inhalt

Über BlackBerry 2FA.....	5
Architektur: BlackBerry 2FA.....	5
Authentifizierungsanforderungen über BlackBerry UEM.....	7
Authentifizierungsantworten über BlackBerry UEM.....	9
Authentifizierungsanforderungen über BlackBerry UEM Cloud.....	12
Authentifizierungsantworten über BlackBerry UEM Cloud.....	14
Durchführen von Upgrades für BlackBerry UEM.....	15
BlackBerry 2FA -Profile.....	15
BlackBerry 2FA für von BlackBerry UEM verwaltete Geräte.....	15
BlackBerry 2FA für nicht von BlackBerry UEM verwaltete Geräte.....	15
OTP-Token.....	16
Vorauthentifizierung und Wiederherstellung.....	16
Direkte Authentifizierung.....	17
Schritte zum Verwalten von BlackBerry 2FA in BlackBerry UEM	18
Systemanforderungen: BlackBerry 2FA.....	19
Benutzer erstellen.....	20
Zuweisen der BlackBerry 2FA-App zu BlackBerry 10-Geräten.....	21
Erstellen oder Ändern eines BlackBerry 2FA-Profiles in der BlackBerry UEM-Version 12.8 oder früher.....	22
Erstellen oder Ändern eines BlackBerry 2FA-Profiles in BlackBerry UEM Cloud oder BlackBerry UEM Version 12.9 oder höher.....	23
Zuweisen eines BlackBerry 2FA-Profiles zu einem Benutzer.....	26
Erstellen eines Aktivierungsprofils für die Registrierung von nicht verwalteten Geräten in BlackBerry 2FA...	26
Zuweisen eines Aktivierungsprofils nur für die Registrierung für Benutzer mit nicht verwalteten Geräten....	27
Aktivieren eines BlackBerry 10-Geräts.....	27
Aktivieren eines iOS-Geräts.....	28
Aktivieren eines Android-Geräts.....	28
Einrichten oder Zurücksetzen einer Vorauthentifizierung.....	29
Schritte für die Verwaltung von OTP-Hardware-Token.....	30
Aktivieren der OTP-Tokenfunktion.....	30
Deaktivieren der OTP-Tokenfunktion.....	30
Unterstützte OTP-Hardware-Token.....	30
Verwenden des BlackBerry 2FA Token Conversion Tool.....	31
Bearbeiten der CSVConfig-Konfigurationsdatei.....	32
Importieren von OTP-Token in BlackBerry UEM.....	33
Entfernen eines OTP-Token aus BlackBerry UEM.....	34
Zuweisen eines OTP-Token zu einem Benutzer.....	34
Entfernen eines OTP-Token von einem Benutzer.....	34
Nicht synchronisierte Hardware-Token automatisch anpassen.....	34
Manuelles erneutes Synchronisieren eines Hardware-Tokens.....	35
Protokollierung und Reporting.....	36

Überwachung von Vorauthentifizierungsanfragen..... 36

Rechtliche Hinweise.....38

Über BlackBerry 2FA

BlackBerry 2FA schützt den Zugang zu den kritischen Ressourcen Ihres Unternehmens mithilfe der Zwei-Faktor-Authentifizierung. Das Produkt verlangt ein Kennwort von Benutzern und zeigt jedes Mal, wenn sie Ressourcen öffnen möchten, eine Sicherheitsaufforderung auf dem Mobilgerät an. BlackBerry 2FA unterstützt zudem die Verwendung von standardbasierten Einmalkennwort-Token (OTP).

Sie verwalten BlackBerry 2FA-Benutzer von der BlackBerry UEM Cloud- oder BlackBerry UEM-Verwaltungskontrolle aus. BlackBerry 2FA kann auch auf Geräten verwendet werden, die nicht über BlackBerry UEM Cloud oder BlackBerry UEM verwaltet werden. BlackBerry 2FA unterstützt iOS- und Android-Geräte, die nur einen BlackBerry Dynamics-Container aufweisen, von Drittanbieter-MDM-Systemen verwaltete Geräte oder nicht verwaltete Geräte.

Mit BlackBerry 2FA können Sie viele unterschiedliche Systeme schützen, wie VPNs, mit RADIUS kompatible Systeme, benutzerdefinierte Anwendungen mit einer REST API und mit SAML kompatible Cloud-Dienste, wenn diese zusammen mit BlackBerry Enterprise Identity verwendet werden.

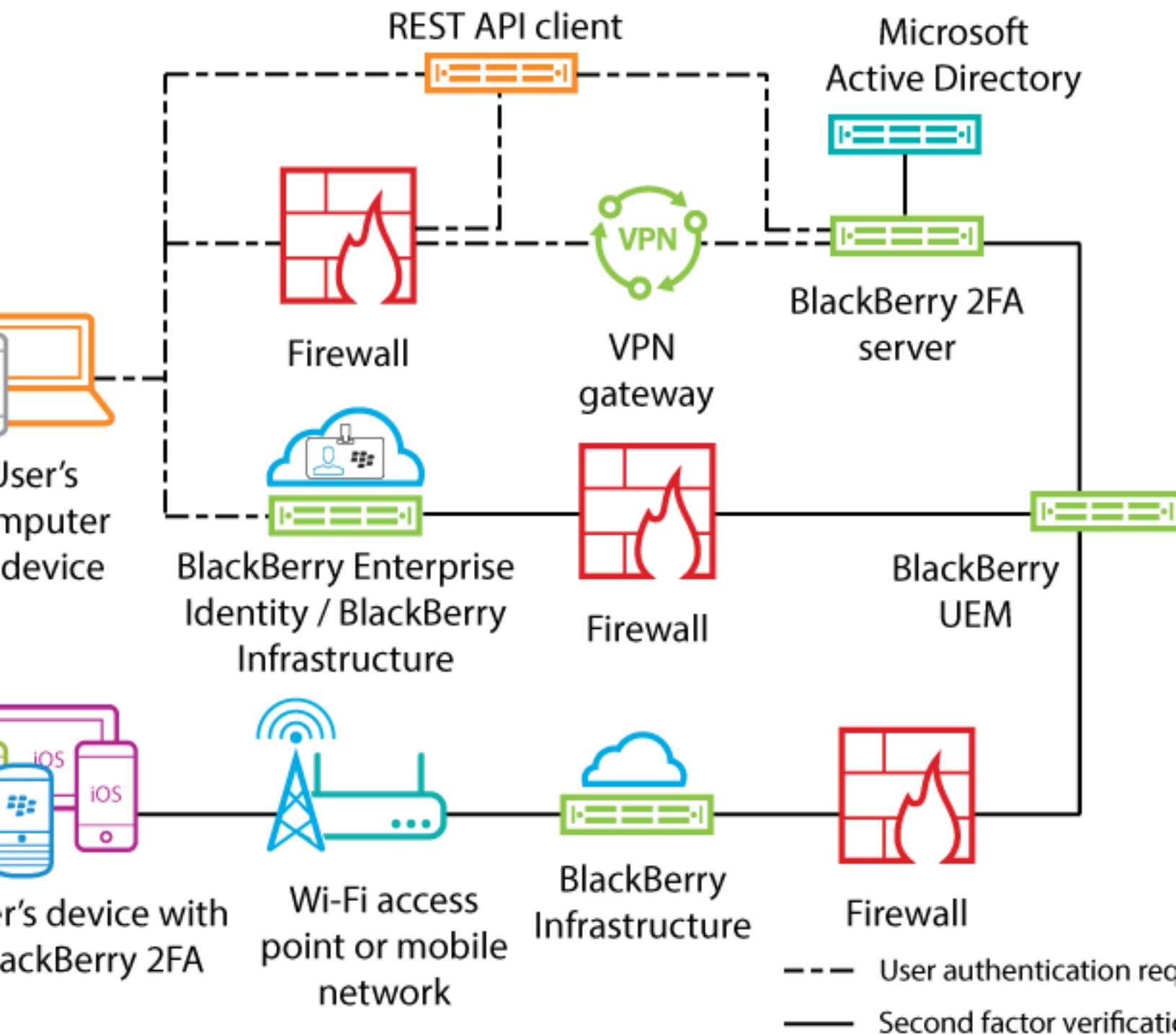
Die Konfiguration von BlackBerry 2FA für die Verwendung mit Mobilgeräten ist unkompliziert. Der erste Authentifizierungsfaktor (das Kennwort) kann ein Benutzerverzeichnis oder das Kennwort eines Containers sein. Der zweite Authentifizierungsfaktor (die Sicherheitsaufforderung) benötigt eine App auf dem Gerät, die eine Sicherheitsbestätigung für das Gerät erzeugt. Bei iOS- und Android-Geräten ist BlackBerry 2FA im BlackBerry UEM Client enthalten. Wenn diese bei der Aktivierung nicht installiert werden, muss die Installation von den Benutzern übernommen werden. Bei Geräten, die von BlackBerry 10 verwaltet werden, muss eine andere BlackBerry 2FA-App eingesetzt oder von den Benutzern installiert werden.

Das Konfigurieren von BlackBerry 2FA für Benutzer ohne Mobilgeräte ist ebenfalls unkompliziert. Standardbasierte OTP-Token werden in der BlackBerry UEM-Konsole registriert und für Benutzer ausgestellt. Die erste Authentifizierungsstufe bildet das Verzeichniskennwort des Benutzers und die zweite Authentifizierungsstufe ein dynamischer Code, der auf dem Token-Bildschirm angezeigt wird. Weitere Informationen finden Sie in der [BlackBerry 2FA-Dokumentation für Administratoren](#).

Der BlackBerry 2FA-Server ist eine optionale Komponente, die eingesetzt wird, wenn das Produkt zusammen mit RADIUS-basierten Systemen verwendet wird, wie die meisten VPNs, oder wenn es mit Apps verwendet wird, die die REST API des Produkts aufrufen. Der BlackBerry 2FA-Server ist bei Bereitstellungen, die nur Enterprise Identity verwenden, nicht erforderlich, kann aber eingesetzt werden, wenn Sie die Zwei-Faktor-Authentifizierung sowohl für die Cloud-Dienste als auch für andere unterstützte Systeme verwenden möchten. Weitere Informationen finden Sie unter [BlackBerry 2FA Server-Kompatibilitätsmatrix](#), [BlackBerry 2FA-Dokumentation zu Serverinstallation und -Upgrade](#) und in der [BlackBerry 2FA-Dokumentation zur Serverkonfiguration](#).

Zur Verwendung von BlackBerry 2FA müssen Sie Benutzerlizenzen für die Collaboration Edition, die Application Edition oder die Content Edition von BlackBerry Enterprise Mobility Suite oder separate 2FA-Benutzerlizenzen erwerben. Bei der Collaboration Edition kann BlackBerry 2FA nur zur Authentifizierung für BlackBerry-Apps und Microsoft Office 365 verwendet werden. Weitere Informationen zu BlackBerry 2FA, einschließlich Informationen zum Erwerb von 2FA, finden Sie unter blackberry.com.

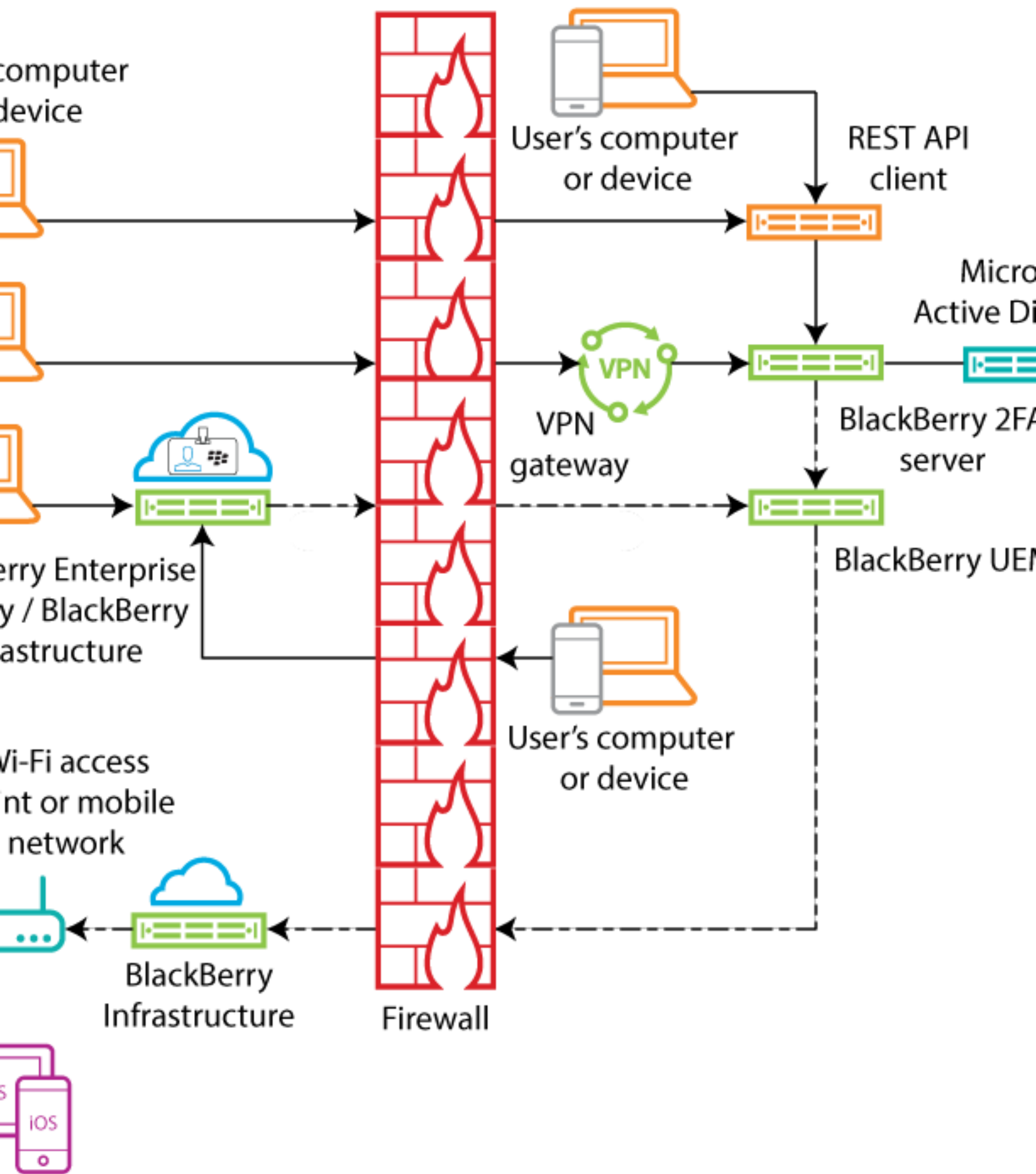
Architektur: BlackBerry 2FA



Komponente	Beschreibung
Computer oder Gerät des Benutzers	Computer oder Geräte des Benutzers können innerhalb oder außerhalb von Firewalls sein, mit denen eine Verbindung zu einer Ressource hergestellt wird, für die eine Zwei-Faktor-Authentifizierung erforderlich ist.

Komponente	Beschreibung
BlackBerry 2FA-Server	Der BlackBerry 2FA-Server stellt eine Verbindung zu BlackBerry UEM her, um die einem Benutzer zugeordneten Geräte zu finden und Authentifizierungsanfragen an die BlackBerry 2FA-App zu senden, die auf den Geräten installiert ist.
VPN-Gateway (optional)	Das VPN-Gateway ist ein Computer, der VPN-Verbindungen mit dem Netzwerk Ihres Unternehmens akzeptiert. Hinweis: Für diese Funktion ist der BlackBerry 2FA-Server erforderlich.
REST API-Client (optional)	Der REST API-Client ist ein benutzerdefinierter Vor-Ort-Dienst, der Benutzer authentifiziert, die darauf über die REST API des BlackBerry 2FA-Servers zugreifen. Hinweis: Für diese Funktion ist der BlackBerry 2FA-Server erforderlich.
BlackBerry Enterprise Identity (optional)	BlackBerry Enterprise Identity ermöglicht den Zugriff per einmaliger Anmeldung (SSO) auf Cloud-Dienste wie Box, Salesforce und G Suite. Enterprise Identity ermöglicht die direkte Verbindung mit dem BlackBerry 2FA-Dienst in BlackBerry UEM oder BlackBerry UEM Cloud.
BES12 oder BlackBerry UEM, BlackBerry UEM Cloud	BlackBerry UEM verwaltet zudem die BlackBerry 2FA-Benutzerkonfiguration über das BlackBerry 2FA-Profil und die Verwendung der Token für Einmalkennwörter (OTP).
Benutzergerät mit BlackBerry 2FA	Bei iOS- und Android-Geräten ist BlackBerry 2FA im BlackBerry UEM Client enthalten. Benutzer mit BlackBerry 10-Geräten installieren die BlackBerry 2FA-App.

Authentifizierungsanforderungen über BlackBerry UEM



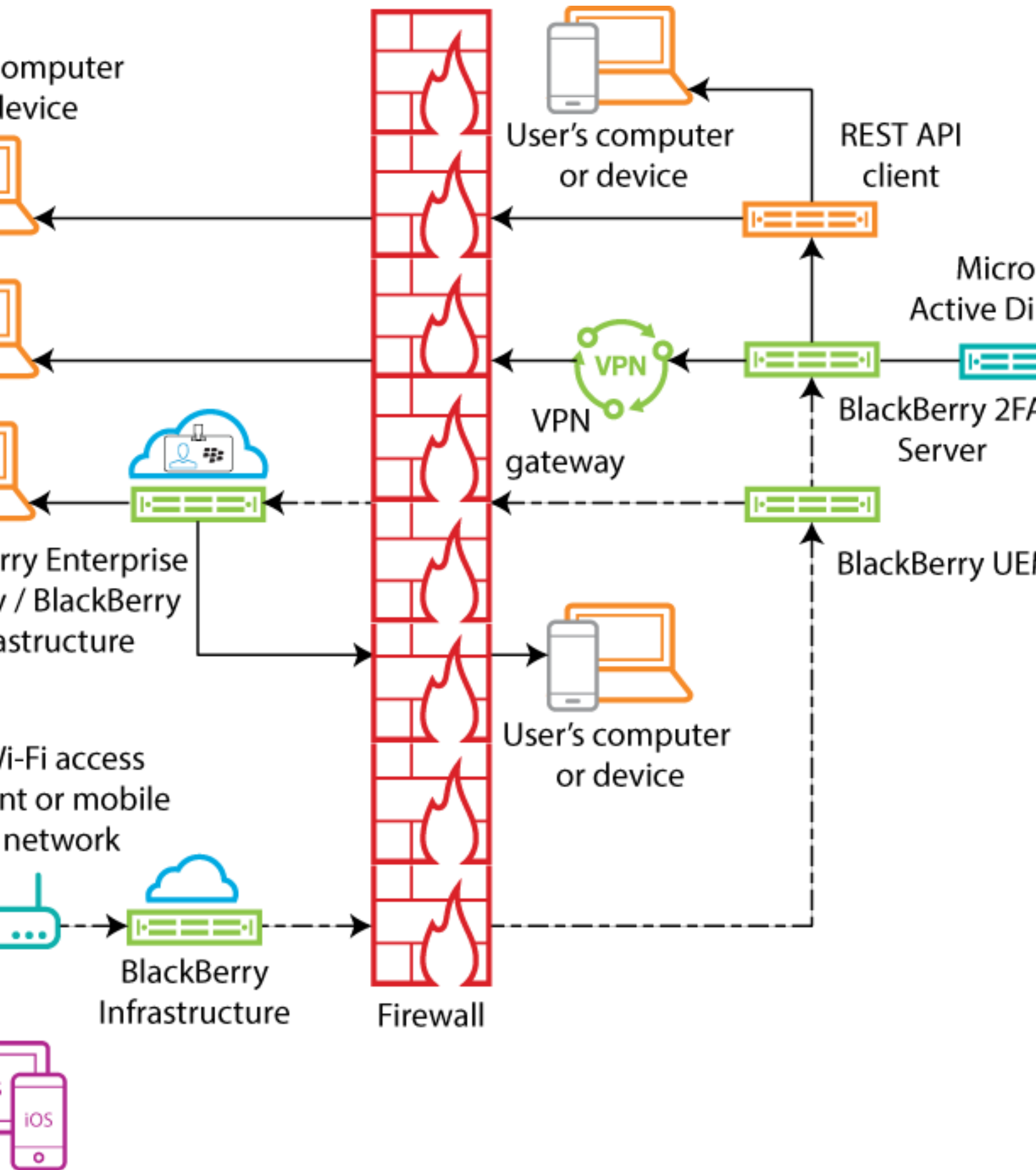
Zum Einleiten einer Authentifizierungsanforderung müssen Benutzer einen der folgenden Schritte ausführen:

- Aufrufen der Schnittstelle für die Anmeldung bei einem benutzerdefinierten Dienst auf einem geschäftlichen Computer oder Gerät und Eingabe der Anmeldeinformationen
- Aufrufen der Schnittstelle für die Anmeldung bei einem benutzerdefinierten Dienst auf einem nicht zum Unternehmen gehörenden Computer oder Gerät und Eingabe der Anmeldeinformationen
- Öffnen eines VPN-Clients auf einem nicht zum Unternehmen gehörenden Computer oder Gerät und Eingabe der Anmeldeinformationen
- Aufrufen der Schnittstelle für die Anmeldung bei einem Dienst, der für die Verwendung von BlackBerry Enterprise Identity bei der Authentifizierung auf einem nicht zum Unternehmen gehörenden Computer oder Gerät konfiguriert wurde, und Eingabe der Anmeldeinformationen
- Aufrufen der Schnittstelle für die Anmeldung bei einem Dienst, der für die Verwendung von BlackBerry Enterprise Identity bei der Authentifizierung auf einem geschäftlichen Computer oder Gerät konfiguriert wurde, und Eingabe der Anmeldeinformationen

Die Benutzer erhalten eine Eingabeaufforderung auf ihrem Gerät, über die sie die Authentifizierung bestätigen können. Je nach den für die Benutzer konfigurierten Authentifizierungsoptionen müssen sie möglicherweise ihr Kennwort für das Gerät oder den sicheren Container eingeben, bevor sie die Eingabeaufforderung bestätigen können.

Das Diagramm zeigt nicht den Datenfluss von Authentifizierungsanforderungen an, bei denen Token für Einmalkennwörter (OTP) verwendet werden.

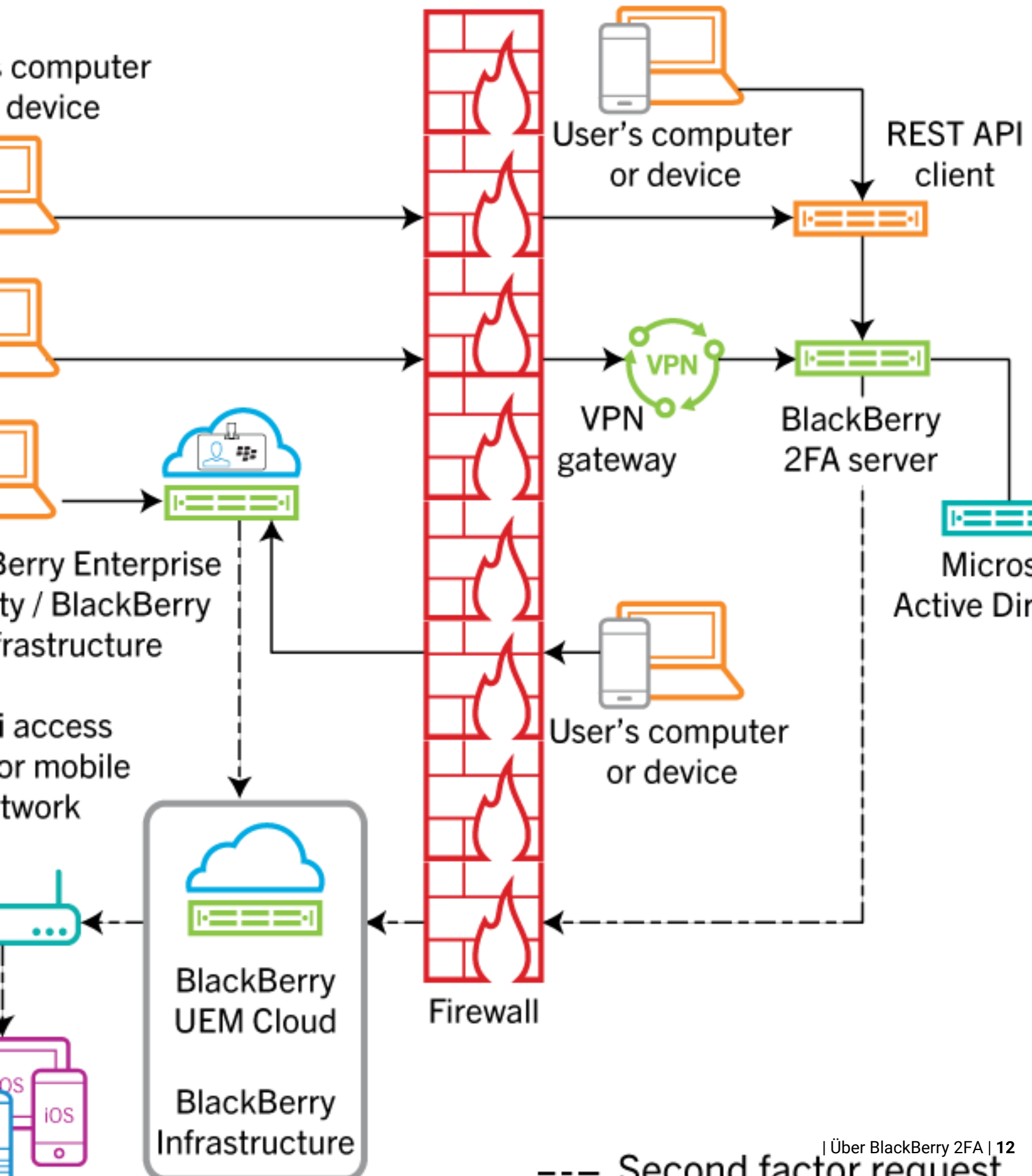
Authentifizierungsantworten über BlackBerry UEM



Bei allen angezeigten Antworten bestätigen die Benutzer die Authentifizierungsaufforderung auf ihrem Gerät, und die Antwort wird an BlackBerry Enterprise Identity oder den BlackBerry 2FA-Server zurückgeleitet. Das Benutzerkennwort für das Verzeichnis wird überprüft, wenn dies aufgrund der für den Benutzer festgelegten Authentifizierungsoptionen erforderlich ist. Nach dem Überprüfen des Kennworts erhalten die Benutzer auf ihrem Gerät die Nachricht, dass die Antwort auf die Eingabeaufforderung erfolgreich versendet wurde.

Das Diagramm zeigt nicht den Datenfluss von Authentifizierungen an, bei denen Token für Einmalkennwörter (OTP) verwendet werden.

Authentifizierungsanforderungen über BlackBerry UEM Cloud



Zum Einleiten einer Authentifizierungsanforderung müssen Benutzer einen der folgenden Schritte ausführen:

- Aufrufen der Schnittstelle für die Anmeldung bei einem Dienst, der für die Verwendung von BlackBerry Enterprise Identity bei der Authentifizierung auf einem nicht zum Unternehmen gehörenden Computer oder Gerät konfiguriert wurde, und Eingabe der Anmeldeinformationen
- Aufrufen der Schnittstelle für die Anmeldung bei einem Dienst, der für die Verwendung von BlackBerry Enterprise Identity bei der Authentifizierung auf einem geschäftlichen Computer oder Gerät konfiguriert wurde, und Eingabe der Anmeldeinformationen

Die Benutzer erhalten eine Eingabeaufforderung auf ihrem Gerät, über die sie die Authentifizierung bestätigen können. Je nach den für die Benutzer konfigurierten Authentifizierungsoptionen müssen sie möglicherweise ihr Kennwort für das Gerät oder den sicheren Container eingeben, bevor sie die Eingabeaufforderung bestätigen können.

Das Diagramm zeigt nicht den Datenfluss von Authentifizierungsanforderungen an, bei denen Token für Einmalkennwörter (OTP) verwendet werden.

Bei allen angezeigten Antworten bestätigen die Benutzer die Authentifizierungsaufforderung auf ihrem Gerät, und die Antwort wird an BlackBerry Enterprise Identity zurückgeleitet. Das Benutzerkennwort für das Verzeichnis wird überprüft, wenn dies aufgrund der für den Benutzer festgelegten Authentifizierungsoptionen erforderlich ist. Nach dem Überprüfen des Kennworts erhalten die Benutzer auf ihrem Gerät die Nachricht, dass die Antwort auf die Eingabeaufforderung erfolgreich versendet wurde.

Das Diagramm zeigt nicht den Datenfluss von Authentifizierungen an, bei denen Token für Einmalkennwörter (OTP) verwendet werden.

Durchführen von Upgrades für BlackBerry UEM

Wenn Sie ein Upgrade für BlackBerry UEM durchführen möchten und einen BlackBerry 2FA-Server verwenden, müssen Sie den BlackBerry 2FA-Dienst auf dem 2FA-Server neu starten. Führen Sie beispielsweise ein Upgrade von BlackBerry UEM-Version 12.6 auf 12.7 aus, und Sie verwenden den BlackBerry 2FA-Server 2.5, müssen Sie den BlackBerry 2FA-Service auf dem 2FA-Server neu starten.

Die neuesten Informationen zur Kompatibilität finden Sie unter [BlackBerry 2FA Server-Kompatibilitätsmatrix](#).

BlackBerry 2FA -Profile

Mit einem BlackBerry 2FA-Profil können Sie die Authentifizierung für Ihre Benutzer aktivieren. Um die aktuelle Version von BlackBerry 2FA und die zugehörigen Funktionen nutzen zu können, z. B. OTP-Tokenunterstützung für Hardware oder Software, direkte BlackBerry 2FA-Authentifizierung, BlackBerry 2FA-Vorauthentifizierung und Wiederherstellung, muss Benutzern das BlackBerry 2FA-Profil zugewiesen werden. Weitere Informationen zum Gebrauch des BlackBerry 2FA-Profiles finden Sie in [Erstellen oder Ändern eines BlackBerry 2FA-Profiles in der BlackBerry UEM-Version 12.8 oder früher](#) und [Zuweisen eines BlackBerry 2FA-Profiles zu einem Benutzer](#). Informationen zur Verwendung von BlackBerry 2FA in BlackBerry UEM finden Sie unter [Schritte zum Verwalten von BlackBerry 2FA in BlackBerry UEM](#).

BlackBerry 2FA für von BlackBerry UEM verwaltete Geräte

Sie können Geräte in BlackBerry UEM aktivieren, sodass Sie diese verwalten und BlackBerry 2FA verwenden können. Eine einzige Aktivierungsaufgabe muss ausgeführt werden, um die MDM-Steuerung sowie BlackBerry 2FA für das Gerät bereitzustellen. Dadurch wird die Geräteverwaltung sowohl für Benutzer als auch für Administratoren vereinfacht.

Alle von BlackBerry UEM unterstützten Aktivierungsprofile ermöglichen die Verwendung von BlackBerry 2FA. Weitere Informationen zur Verwendung von BlackBerry 2FA in BlackBerry UEM finden Sie in der [BlackBerry 2FA-Dokumentation für Administratoren](#).

BlackBerry 2FA für nicht von BlackBerry UEM verwaltete Geräte

Wenn die Verwaltung über BlackBerry UEM nicht möglich ist oder ein Gerät bereits über eine andere MDM-Lösung verwaltet wird, können Sie Geräte mit BlackBerry UEM aktivieren, sodass diese nur BlackBerry 2FA verwenden.

Geräte, die auf diese Weise aktiviert werden, können nicht über BlackBerry UEM verwaltet werden. Es wird kein geschäftlicher Bereich auf den Geräten erstellt, keine administrative Kontrolle für das Gerät eingerichtet, es gibt keinen zusätzlichen Schutz für geschäftliche Daten und die persönlichen Daten von Benutzern bleiben privat.

Diese Option steht nur für iOS- und Android-Geräte zur Verfügung. Weitere Informationen zur Verwendung von BlackBerry 2FA in BlackBerry UEM finden Sie in der [BlackBerry 2FA-Dokumentation für Administratoren](#).

OTP-Token

BlackBerry UEM unterstützt die Verwendung von Einmalkennwort-Token (OTP) über den BlackBerry 2FA-Dienst. Die OTP-Tokenfunktion stellt ein sicheres Authentifizierungsschema für Benutzer bereit, die kein Mobilgerät oder ein Mobilgerät ohne ausreichende Konnektivität für die Unterstützung der Echtzeit-Gerätebenachrichtigungen von BlackBerry 2FA nutzen. Bei Verwendung von OTP anstelle der Gerätebenachrichtigung als zweite Authentifizierungsstufe erfolgt die OTP-Bereitstellung über denselben Kanal wie das Kennwort des Benutzers, ohne dass ein Signal an das Mobilgerät gesendet wird.

Sie können den OTP-Code mit dem Benutzernamen oder dem Kennwort eingeben.

- Bei Verwendung eines OTP-Codes mit dem Benutzernamen geben Sie nach dem Benutzernamen ohne Leerzeichen dazwischen ein Komma (,) und dann den OTP-Code ein. Lautet der Benutzername beispielsweise „janedoe“ und der Code „555123“, so muss die Zeichenfolge „janedoe,555123“ eingegeben werden. Mit dieser Methode können Benutzer auf einfache Weise den von ihnen eingegebenen Code überprüfen.
- Wenn Sie einen OTP-Code mit dem Kennwort verwenden, ist der Code dem Kennwort des Benutzers vorangestellt. Lautet der Code beispielsweise „555123“ und das Kennwort „AbCdeF“, muss die Zeichenfolge „555123AbCdeF“ eingegeben werden.

Software-Token

Sie aktivieren OTP-Token für Benutzer in dem BlackBerry 2FA-Profil, das Sie diesen zuweisen. Das Software-Token können Sie in der BlackBerry UEM Client-App anzeigen, indem Sie über den Startbildschirm wischen.

Hardware-Token

Zur Verwaltung von Hardware-OTP-Token in BlackBerry UEM muss dem Benutzer ein BlackBerry 2FA-Profil zugewiesen werden.

Weitere Informationen zu den letzten unterstützten Hardware-Token finden Sie in der [BlackBerry 2FA-Server-Kompatibilitätsmatrix](#).

Vorauthentifizierung und Wiederherstellung

Bei der BlackBerry 2FA-Vorauthentifizierung und der Wiederherstellung handelt es sich um Funktionen, die Benutzern die Authentifizierung bei den Ressourcen Ihres Unternehmens mit nur einem Faktor innerhalb eines vordefinierten Zeitraums ermöglichen. Diese Funktionen werden unabhängig voneinander aktiviert und konfiguriert.

Vorauthentifizierung muss verwendet werden, wenn Benutzer davon ausgehen können, dass sie über einen kurzen Zeitraum keinen Zugang zum Gerät haben oder über keine Netzabdeckung verfügen (z. B. in einem Flugzeug). Benutzer können eine Vorauthentifizierung über ihr Gerät anfordern, oder Administratoren können diese Funktion über die BlackBerry UEM-Verwaltungskonsole aktivieren. BlackBerry empfiehlt stattdessen nach Möglichkeit eine Verwendung der OTP-Funktion der Software, da hiermit die vollständige Zwei-Faktor-Sicherheit gewährleistet wird, auch wenn diese Funktion weniger benutzerfreundlich ist.

Wiederherstellung sollte verwendet werden, wenn Benutzer ihr Gerät verloren oder über einen längeren Zeitraum, z. B. einen Tag oder länger, keinen Zugriff auf das Gerät haben (wenn ein Benutzer beispielsweise sein Gerät verloren hat und auf ein Ersatzgerät wartet). Benutzer können auf die Wiederherstellungsfunktion über BlackBerry

UEM Self-Service zugreifen. Das bedeutet, dass diese nur aktiviert werden kann, wenn der Benutzer mit dem Netzwerk des Unternehmens verbunden ist.

Direkte Authentifizierung

Sie können die direkte BlackBerry 2FA-Authentifizierung aktivieren, sodass Benutzer beim Authentifizieren bei den Ressourcen Ihres Unternehmens den Authentifizierungsvorgang über ihre Geräte starten können, anstatt eine Bestätigungsaufforderung zu erhalten; zudem benötigen sie kein Einmalkennwort. Wenn Sie die Funktion zur direkten Authentifizierung für Benutzer aktivieren, müssen diese ihr Verzeichniskennwort verwenden, um sich bei den Ressourcen ihres Unternehmens innerhalb des von Ihnen vorgegebenen Zeitlimits anzumelden.

Benutzer können auf die Funktion der direkten Authentifizierung vom BlackBerry UEM Client auf Android- und iOS-Geräten und über die BlackBerry 2FA-App auf BlackBerry 10-Geräten zugreifen.

Schritte zum Verwalten von BlackBerry 2FA in BlackBerry UEM

Um BlackBerry UEM zum Verwalten von BlackBerry 2FA zu verwenden, müssen Sie die folgenden Schritte ausführen:

Schritt	Aktion
1	Vergewissern Sie sich, dass Ihre Umgebung die Anforderungen an Geräte und Server erfüllt. Weitere Informationen finden Sie unter Systemanforderungen: BlackBerry 2FA .
2	Optional können Sie den BlackBerry 2FA-Server installieren und konfigurieren. Weitere Informationen finden Sie in der Dokumentation zur Installation und Konfiguration .
3	Benutzer erstellen.
4	Zuweisen der BlackBerry 2FA-App zu BlackBerry 10-Geräten.
5	Erstellen oder Ändern eines BlackBerry 2FA-Profiles in der BlackBerry UEM-Version 12.8 oder früher oder Erstellen oder Ändern eines BlackBerry 2FA-Profiles in BlackBerry UEM Cloud oder BlackBerry UEM Version 12.9 oder höher.
6	Zuweisen eines BlackBerry 2FA-Profiles zu einem Benutzer.
7	Optional Erstellen eines Aktivierungsprofils für die Registrierung von nicht verwalteten Geräten in BlackBerry 2FA.
8	Optional Zuweisen eines Aktivierungsprofils nur für die Registrierung für Benutzer mit nicht verwalteten Geräten.
9	Aktivieren eines BlackBerry 10-Geräts.
10	Aktivieren eines iOS-Geräts.
11	Aktivieren eines Android-Geräts.
12	Einrichten oder Zurücksetzen einer Vorauthentifizierung.
13	Konfigurieren Sie ggf. BlackBerry UEM für die Verwendung von Einmalkennwort-Token (OTP). Weitere Informationen finden Sie unter Schritte für die Verwaltung von OTP-Hardware-Token .

Systemanforderungen: BlackBerry 2FA

Bevor Sie BlackBerry UEM zum Verwalten von BlackBerry 2FA verwenden können, müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind:

Objekt	Anforderungen
BlackBerry UEM oder BlackBerry UEM Cloud	<p>Eine der folgenden Bedingungen muss erfüllt sein:</p> <ul style="list-style-type: none">• BlackBerry UEM Version 12.6 oder höher• BlackBerry UEM Cloud <p>Weitere Informationen zur Installation von BlackBerry UEM 12.6 oder höher finden Sie in der BlackBerry UEM-Dokumentation zu Installation und Upgrade.</p>
BlackBerry 2FA-Server	<ul style="list-style-type: none">• Version 2.0 oder höher (Version 2.5 für die vollständige Integration aller neuen BlackBerry UEM-Funktionen, einschließlich OTP-Token) <p>Weitere Informationen zu den Systemanforderungen finden Sie in der BlackBerry 2FA-Dokumentation zur Kompatibilitätsmatrix</p> <p>Hinweis: Zur Verwaltung des BlackBerry 2FA-Servers über die BlackBerry UEM-Verwaltungskonsole ist die Version 2.5 des BlackBerry 2FA-Servers erforderlich.</p>
BlackBerry 2FA-Lizenzen	<ul style="list-style-type: none">• BlackBerry 2FA ist in der BlackBerry Enterprise Mobility Suite - Application Edition und in der BlackBerry Enterprise Mobility Suite - Content Edition enthalten und kann auch separat erworben werden.• BlackBerry 2FA ist in der BlackBerry Enterprise Mobility Suite - Collaboration Edition enthalten und ausschließlich für die Authentifizierung mit Microsoft Office 365 und proprietären BlackBerry Unternehmensprodukten vorgesehen.• BlackBerry 2FA ist in allen eigenständigen BlackBerry Workspaces-Lizenzen enthalten und ausschließlich für die Authentifizierung mit Workspaces vorgesehen.• Wenden Sie sich an Ihren BlackBerry-Kundenbetreuer, um die aktuellsten Informationen zu Softwarepaketen, Preisen und Lizenzen zu erhalten.
BlackBerry 10	<ul style="list-style-type: none">• Alle Versionen. Weitere Informationen finden Sie in der BlackBerry 2FA-Dokumentation zur Kompatibilitätsmatrix.
iOS	<ul style="list-style-type: none">• iOS Version 8 und höher Weitere Informationen finden Sie in der BlackBerry 2FA-Dokumentation zur Kompatibilitätsmatrix.• Die aktuelle Version von BlackBerry UEM Client ist installiert. Weitere Informationen finden Sie in der BlackBerry UEM-Dokumentation für Administratoren.
Android	<ul style="list-style-type: none">• Android Version 4.0.x und höher. Weitere Informationen finden Sie in der BlackBerry 2FA-Dokumentation zur Kompatibilitätsmatrix.• Die aktuelle Version von BlackBerry UEM Client ist installiert. Weitere Informationen finden Sie in der Dokumentation für BlackBerry UEM-Administratoren.

Objekt	Anforderungen
Gerätelizenzen	Für Geräte, die BlackBerry 2FA verwenden, aber nicht von BlackBerry UEM verwaltet werden, sind keine Lizenzen erforderlich.


Benutzer erstellen

Jeder BlackBerry 2FA-Benutzer muss als Benutzer in BlackBerry UEM vorhanden sein. Führen Sie einen der folgenden Schritte aus:

- Wenn der Benutzer bereits in BlackBerry UEM vorhanden ist, befolgen Sie die Anweisungen zum Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail in [BlackBerry UEM – Dokumentation für Administratoren](#).
- Wenn der Benutzer in BlackBerry UEM noch nicht vorhanden ist, befolgen Sie die nachfolgenden Schritte, um einen zu erstellen und dem Benutzer ein Aktivierungskennwort zu senden.

Um die erweiterte Version dieser Aufgabe auszuführen, befolgen Sie die Anweisungen in der [Dokumentation für BlackBerry UEM-Administratoren](#), um ein Benutzerkonto zu erstellen.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Benutzer**.
2. Klicken Sie im linken Fensterbereich auf **Benutzer hinzufügen**.
3. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Hinzufügen eines Verzeichnisbenutzers	<ol style="list-style-type: none"> a. Geben Sie auf der Registerkarte Unternehmensverzeichnis im Suchfeld die Suchkriterien für den Verzeichnisbenutzer an, den Sie hinzufügen möchten. Sie können nach Vorname, Nachname, Anzeigename, Benutzername oder E-Mail-Adresse suchen. b. Klicken Sie auf . c. Wählen Sie in den Suchergebnissen das Benutzerkonto aus.
Hinzufügen eines lokalen Benutzers	<ol style="list-style-type: none"> a. Klicken Sie auf die Registerkarte Lokal. b. Geben Sie den Vornamen und den Nachnamen für das Benutzerkonto ein. c. Nehmen Sie im Feld Anzeigename bei Bedarf die gewünschten Änderungen vor. Der Anzeigename wird automatisch anhand des von Ihnen angegebenen Vor- und Nachnamens konfiguriert. d. Geben Sie im Feld Benutzername einen eindeutigen Benutzernamen für das Benutzerkonto ein. e. Geben Sie im Feld E-Mail-Adresse eine Kontakt-E-Mail-Adresse für das Benutzerkonto ein. Die E-Mail-Adresse für das Benutzerkonto ist erforderlich, wenn Sie einen Dienst wie BlackBerry Workspaces oder die Geräteverwaltung aktivieren. f. Geben Sie im Feld Konsolenkennwort ein Kennwort für BlackBerry UEM Self-Service ein. Wenn der Benutzer einer Administratorrolle zugeordnet ist, können Sie auch das Kennwort für den Zugriff auf die Verwaltungskonsole verwenden.

4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Generieren Sie automatisch ein Aktivierungskennwort für den Benutzer, und senden Sie eine Aktivierungs-E-Mail.	<ol style="list-style-type: none"> Aktivieren Sie die Option Automatisch ein Geräteaktivierungskennwort generieren und eine E-Mail mit Aktivierungsanweisungen senden. Legen Sie im Feld Ablauf des Aktivierungszeitraums die Anzahl der Minuten, Stunden oder Tage fest, innerhalb derer ein Benutzer ein Gerät vor Ablauf des Aktivierungskennworts aktivieren kann. Klicken Sie in der Dropdown-Liste Vorlage für Aktivierungs-E-Mails auf eine Vorlage für die Aktivierungs-E-Mail.
Definieren Sie ein Kennwort für den Benutzer, und senden Sie ggf. eine Aktivierungs-E-Mail.	<ol style="list-style-type: none"> Aktivieren Sie die Option Geräteaktivierungskennwort festlegen. Geben Sie ein Aktivierungskennwort ein. Legen Sie im Feld Ablauf des Aktivierungszeitraums die Anzahl der Minuten, Stunden oder Tage fest, innerhalb derer ein Benutzer ein Gerät vor Ablauf des Aktivierungskennworts aktivieren kann. Führen Sie eine der folgenden Aktionen aus: <ol style="list-style-type: none"> Um die Aktivierungsanweisungen an den Benutzer zu senden, klicken Sie in der Dropdown-Liste Aktivierungs-E-Mail-Vorlage auf eine Vorlage zur Verwendung für die Aktivierungs-E-Mail. Wenn Sie keine Aktivierungsanweisungen an den Benutzer senden möchten, deaktivieren Sie das Kontrollkästchen E-Mail mit Aktivierungsanweisungen und Aktivierungskennwort senden. Sie müssen das Aktivierungskennwort dem Benutzer mitteilen.
Richten Sie kein Aktivierungskennwort für den Benutzer ein.	<ol style="list-style-type: none"> Aktivieren Sie die Option Aktivierungskennwort für das Gerät nicht festlegen. Sie können ein Aktivierungskennwort festlegen und die Aktivierungs-E-Mail später senden.

- Wenn Sie benutzerdefinierte Variablen verwenden, erweitern Sie den Punkt **Benutzerdefinierte Variablen**, und geben Sie die entsprechenden Werte für die definierten Variablen ein.
- Führen Sie eine der folgenden Aktionen aus:
 - Um den Benutzer zu speichern, klicken Sie auf **Speichern**.
 - Um den Benutzer zu speichern und ein weiteres Benutzerkonto zu erstellen, klicken Sie auf **Speichern und neu**.

Zuweisen der BlackBerry 2FA-App zu BlackBerry 10-Geräten

Sie müssen die folgenden Aufgaben ausführen, um die App BlackBerry 10-Geräten zuzuweisen, wenn Sie BlackBerry UEM verwenden. Weitere Informationen über die Zuweisung von Apps finden Sie in der [Dokumentation für BlackBerry UEM-Administratoren](#).



- Laden Sie die App von <https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B> herunter, und kopieren Sie die BAR-Datei in ein Verzeichnis, auf das die BlackBerry UEM-Verwaltungskonsole zugreifen kann.
- Verwenden Sie ggf. die BlackBerry UEM-Verwaltungskonsole, um einen freigegebenen Netzwerkpfad für interne Apps anzugeben.

3. Fügen Sie die .bar-Datei in der BlackBerry UEM-Verwaltungskonsole als interne App hinzu.
4. Weisen Sie die App in der BlackBerry UEM-Verwaltungskonsole einem Benutzer oder einer Gruppe zu.

Die App wird automatisch auf allen BlackBerry 10-Geräten installiert, die der Benutzer mit einem Workspace aktiviert.

Erstellen oder Ändern eines BlackBerry 2FA-Profiles in der BlackBerry UEM-Version 12.8 oder früher

Zur Verwendung von BlackBerry 2FA müssen Sie ein BlackBerry 2FA-Profil erstellen und dieses Benutzern zuweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > BlackBerry 2FA**.
3. Führen Sie einen der folgenden Schritte aus:
 - Um ein Profil zu erstellen, klicken Sie auf .
 - Um ein Profil zu ändern, klicken Sie auf den Namen des Profils, das Sie ändern möchten, und klicken Sie auf .
4. Geben Sie einen Namen für das BlackBerry 2FA-Profil ein.
5. Fügen Sie ggf. eine Beschreibung für das BlackBerry 2FA-Profil hinzu.
6. Wählen Sie eine Authentifizierungsoption:
 - a) Wählen Sie **Zwei-Faktor-Authentifizierung**, wenn Sie ein BlackBerry 2FA-Standardprofil erstellen.
 - b) Wählen Sie **Ein-Faktor-Authentifizierung mittels Unternehmenskennwort**, wenn Sie ein Profil für Benutzer erstellen, die kein Gerät haben, aber Zugriff auf die Ressourcen Ihres Unternehmens benötigen. Diese Option bietet weniger Sicherheit, da der Benutzer nur bei Anforderung der Authentifizierung ein Verzeichniskennwort bereitstellt und keine Bestätigungsaufforderung für die Authentifizierung gesendet wird. OTP-Token (Token für Einmalkennwort) werden bei dieser Option nicht unterstützt.
7. Wählen Sie ein Kennwort aus, das bei Eingabeaufforderung durch das Gerät verwendet werden soll:
 - a) Wählen Sie **Enterprise-Kennwort**, wenn Sie ein Profil für Benutzer erstellen, die bei Authentifizierungsanforderung zunächst ihr Verzeichniskennwort eingeben müssen und dann eine Bestätigungsaufforderung auf ihrem Gerät erhalten.
 - b) Wählen Sie **Passives Gerätekenwort**, wenn Sie ein Profil für BlackBerry 10-Benutzer erstellen, die eine passive Aufforderung zur Eingabe ihres Arbeitsbereichskennworts sowie zum Entsperren ihres Arbeitsbereichs und dann eine Bestätigungsaufforderung für die Authentifizierung auf ihren Geräten erhalten sollen. Passive Eingabeaufforderung bedeutet, dass der Benutzer kein Kennwort für den Arbeitsbereich eingeben muss, wenn er eine Authentifizierung anfordert und der Arbeitsbereich des Geräts bereits entsperrt ist.
 - c) Wählen Sie **Aktives Gerätekenwort**, wenn Sie ein Profil für BlackBerry 10-Benutzer erstellen, die eine aktive Aufforderung zur Eingabe ihres Arbeitsbereichskennworts sowie zum Entsperren ihres Arbeitsbereichs und dann eine Bestätigungsaufforderung für die Authentifizierung auf ihren Geräten erhalten sollen. Aktive Eingabeaufforderung bedeutet, dass der Benutzer ein Kennwort für den Arbeitsbereich eingeben muss, wenn er eine Authentifizierung anfordert und der Arbeitsbereich des Geräts bereits entsperrt ist.
8. Optional: Falls Sie die Authentifizierungsrichtlinie **Unternehmenskennwort** verwenden, führen Sie einen der folgenden Schritte aus:
 - a) Um Benutzern in der BlackBerry UEM Client-App die Verwendung von OTPs zu erlauben, wählen Sie **Token für Einmalkennwort zulassen** aus. Legen Sie die Länge der zu generierenden OTPs fest.
 - b) Wählen Sie die Option **Direkte Authentifizierung über Benutzergerät zulassen** aus, damit die Benutzer eine direkte Authentifizierung anfordern können. Legen Sie die Dauer in Sekunden fest, die Benutzern für


die Zwei-Faktor-Authentifizierung zur Verfügung steht, nachdem sie den Vorgang auf ihrem mobilen Gerät gestartet haben. Der Höchstwert für diese Einstellung beträgt „180“.

- c) Wählen Sie die Option **Wiederherstellung über BlackBerry UEM Self-Service zulassen** aus, damit die Benutzer einen Wiederherstellungszeitraum festlegen können. Geben Sie einen Standard- und einen maximalen Zeitraum in Stunden an, in dem Benutzer auf die Ressourcen Ihres Unternehmens Zugriff haben, ohne auf eine Bestätigungsaufforderung auf deren Geräten antworten zu müssen.
- d) Wählen Sie die Option **Vorauthentifizierung über Benutzergerät zulassen** aus, damit die Benutzer einen Vorauthentifizierungszeitraum festlegen können. Geben Sie einen Standard- und einen maximalen Zeitraum in Stunden an, in dem Benutzer auf die Ressourcen Ihres Unternehmens Zugriff haben, ohne auf eine Bestätigungsaufforderung auf ihren Geräten antworten zu müssen (es wird keine Eingabeaufforderung angezeigt).

9. Klicken Sie auf **Hinzufügen** oder auf **Speichern**.

Erstellen oder Ändern eines BlackBerry 2FA-Profiles in BlackBerry UEM Cloud oder BlackBerry UEM Version 12.9 oder höher

Zur Verwendung von BlackBerry 2FA müssen Sie ein BlackBerry 2FA-Profil erstellen und dieses Benutzern zuweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > BlackBerry 2FA**.
3. Führen Sie einen der folgenden Schritte aus:
 - Um ein Profil zu erstellen, klicken Sie auf **+**.
 - Um ein Profil zu ändern, klicken Sie auf den Namen des Profils, das Sie ändern möchten, und klicken Sie auf .
4. Geben Sie einen Namen für das BlackBerry 2FA-Profil ein.
5. Fügen Sie ggf. eine Beschreibung für das BlackBerry 2FA-Profil hinzu.
6. Führen Sie einen der folgenden Schritte aus:
 - a) Wählen Sie **Authentifizierung mit BlackBerry 2FA**, wenn Sie ein BlackBerry 2FA-Standardprofil erstellen.
 - b) Wählen Sie **Authentifizierung nur mittels Unternehmenskennwort**, wenn Sie ein Profil für Benutzer erstellen, die kein Gerät haben, aber Zugriff auf die Ressourcen Ihres Unternehmens benötigen. Diese Option bietet weniger Sicherheit, da der Benutzer nur bei Anforderung der Authentifizierung ein Verzeichniskennwort bereitstellt und keine Bestätigungsanforderung für die Authentifizierung gesendet wird. OTP-Token (Token für Einmalkennwort) werden bei dieser Option nicht unterstützt.
7. Wenn Sie den Authentifizierungsmodus „Authentifizierung mit BlackBerry 2FA“ ausgewählt haben, konfigurieren Sie die folgenden Einstellungen:

Einstellung	Beschreibung
Push-Authentifizierung zulassen	Diese Einstellung gibt an, ob Benutzern ermöglicht werden soll, sich mithilfe der 2FA-Bestätigungsaufforderung auf ihrem Gerät zu authentifizieren.
Unternehmenskennwort erforderlich	Diese Einstellung gibt an, ob Benutzer ihr Unternehmenskennwort bei der Anmeldung bei den Ressourcen ihres Unternehmens angeben müssen. Nachdem ein Benutzer sein Kennwort eingegeben hat,

Einstellung	Beschreibung
	<p>wird er dazu aufgefordert, sich auf seinem Gerät zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Push-Authentifizierung zulassen“ ausgewählt ist.</p>
<p>Vorauthentifizierung über Mobilgeräte zulassen</p>	<p>Diese Einstellung gibt an, ob Benutzer die Vorauthentifizierungsfunktion verwenden können, um sich bei den Ressourcen Ihres Unternehmens für einen kurzen, begrenzten Zeitraum zu authentifizieren. Wenn Sie diese Option auswählen, ist die Funktion auf dem Startbildschirm der BlackBerry UEM Client-App für die Benutzer verfügbar.</p> <p>Geben Sie die Standard- und maximale Zeitspanne in Stunden an, während der Benutzer auf die Ressourcen Ihres Unternehmens zugreifen können, ohne nach einer Authentifizierung auf ihren Geräten gefragt zu werden.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Push-Authentifizierung zulassen“ und „Unternehmenskennwort erforderlich“ ausgewählt ist.</p>
<p>Gerätekenwort erforderlich, falls Gerät gesperrt ist</p>	<p>Diese Einstellung legt fest, ob die Benutzer ihr Gerät entsperren müssen, bevor sie auf die Authentifizierungsaufforderung auf dem Gerät reagieren können.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Push-Authentifizierung zulassen“ ausgewählt ist.</p>
<p>Erneute Eingabe des Gerätekennworts erforderlich, auch wenn das Gerät bereits entsperrt ist (nur BlackBerry 10-Geräte)</p>	<p>Diese Einstellung legt fest, ob die Benutzer von BlackBerry 10-Geräten ihr Gerätekenwort eingeben müssen, auch wenn das Gerät bereits entsperrt ist, bevor sie auf die Authentifizierungsaufforderung auf dem Gerät reagieren können.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Push-Authentifizierung zulassen“ und „Gerätekenwort erforderlich, falls Gerät gesperrt ist“ ausgewählt ist.</p>
<p>Direkte Authentifizierung über Mobilgeräte zulassen</p>	<p>Diese Einstellung gibt an, ob Benutzer die Funktion für die direkte Authentifizierung verwenden können, um die Authentifizierung auf dem Mobilgerät zu starten. Wenn Sie diese Option auswählen, ist die Funktion auf dem Startbildschirm der BlackBerry UEM Client-App für die Benutzer verfügbar.</p> <p>Sie müssen die Zeitspanne in Sekunden angeben, während die Benutzer die Zwei-Faktor-Authentifizierung abschließen müssen. Die</p>

Einstellung	Beschreibung
	<p>Voreinstellung ist „120“ und die maximale Einstellung ist „180“.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Push-Authentifizierung zulassen“ ausgewählt ist.</p>
Authentifizierung mit Einmalkennwort (OTP) zulassen	<p>Diese Einstellung gibt an, ob Benutzer OTP-Codes als zweiten Faktor für die Authentifizierung verwenden können.</p>
Unternehmenskennwort erforderlich	<p>Diese Einstellung gibt an, ob der Benutzer das Verzeichniskennwort zusammen mit dem OTP-Code eingeben muss.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Authentifizierung mit Einmalkennwort (OTP) zulassen“ ausgewählt ist.</p>
Erstellung eines OTP auf Mobilgeräten zulassen	<p>Diese Einstellung gibt an, ob OTP-Codes auf dem Mobilgerät generiert werden müssen. Wenn Sie diese Option auswählen, können Benutzer OTP-Codes verwenden, die auf dem Startbildschirm der BlackBerry UEM Client-App angezeigt werden.</p> <p>Geben Sie die Länge der OTP-Codes an, die in UEM Client generiert werden sollen. Die Standardlänge ist „6“.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Authentifizierung mit Einmalkennwort (OTP) zulassen“ ausgewählt ist.</p>
OTP-Hardware-Token zulassen	<p>Diese Einstellung gibt an, ob Benutzer OTP-Hardware-Token verwenden dürfen. Wenn Sie diese Option aktivieren, können Benutzer OTP-Codes auf den Hardware-Token verwenden, die ihnen zugewiesen sind.</p> <p>Diese Einstellung ist nur dann gültig, wenn „Authentifizierung mit Einmalkennwort (OTP) zulassen“ ausgewählt ist.</p>
Wiederherstellung von BlackBerry UEM Self-Service zulassen	<p>Diese Einstellung gibt an, ob Benutzer die Wiederherstellungsfunktion verwenden können, um sich bei den Ressourcen Ihres Unternehmens für einen begrenzten Zeitraum zu authentifizieren. Wenn Sie diese Option aktivieren, können Benutzer auf die Wiederherstellungsfunktion in BlackBerry UEM Self-Service zugreifen, aber nur, wenn sie mit dem Netzwerk des Unternehmens verbunden sind.</p> <p>Geben Sie die Standard- und maximale Zeitspanne in Stunden an, während der Benutzer auf die Ressourcen Ihres Unternehmens zugreifen können,</p>

Einstellung	Beschreibung
	ohne nach einer Authentifizierung auf ihren Geräten gefragt zu werden.

8. Klicken Sie auf **Hinzufügen** oder auf **Speichern**.

Zuweisen eines BlackBerry 2FA-Profiles zu einem Benutzer

Der Benutzer muss über ein zugewiesenes BlackBerry 2FA-Profil verfügen, um BlackBerry 2FA nutzen zu können.

Bevor Sie beginnen:

- [Erstellen oder Ändern eines BlackBerry 2FA-Profiles in der BlackBerry UEM-Version 12.8 oder früher.](#)
 - [Erstellen oder Ändern eines BlackBerry 2FA-Profiles in BlackBerry UEM Cloud oder BlackBerry UEM Version 12.9 oder höher.](#)
1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer**.
 2. Suchen Sie nach einem Benutzer.
 3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzers.
 4. Klicken Sie im Abschnitt **IT-Richtlinien und -Profile** auf **+**.
 5. Klicken Sie auf **BlackBerry 2FA**.
 6. Klicken Sie in der Dropdown-Liste **BlackBerry 2FA-Profil** auf ein BlackBerry 2FA-Profil.
 7. Wenn der in Schritt 6 ausgewählte Profiltyp dem Benutzer bereits direkt zugewiesen ist, klicken Sie auf **Ersetzen**. Klicken Sie andernfalls auf **Zuweisen**.

Erstellen eines Aktivierungsprofils für die Registrierung von nicht verwalteten Geräten in BlackBerry 2FA

Führen Sie die folgenden Aufgaben aus, um ein Aktivierungsprofil für Benutzer zu erstellen, deren Geräte nicht von BlackBerry UEM verwaltet werden. Die Geräte müssen über BlackBerry UEM registriert werden, damit sie in BlackBerry 2FA verwendet werden können. Diese Aktivierungsart gilt nur für iOS- und Android-Geräte.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf **+** neben **Aktivierung**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Geben Sie im Feld **Anzahl der Geräte, die ein Benutzer aktivieren kann** die maximale Anzahl von Geräten ein, die der Benutzer aktivieren kann.
5. Führen Sie in der Dropdown-Liste **Geräteigentümer** eine der folgenden Aktionen aus:
 - Wenn einige Benutzer persönliche Geräte und einige Benutzer geschäftliche Geräte aktivieren, wählen Sie **Nicht angegeben** aus.
 - Wenn Benutzer in der Regel geschäftliche Geräte aktivieren, wählen Sie **Geschäftlich** aus.
 - Wenn Benutzer in der Regel persönliche Geräte aktivieren, wählen Sie **Persönlich** aus.
6. Wählen Sie optional einen Organisationshinweis in der Dropdown-Liste **Organisationshinweis zuweisen** aus. Wenn Sie einen Organisationshinweis zuordnen, müssen Benutzer, die iOS-Geräte aktivieren möchten, den Hinweis zum Abschließen der Aktivierung akzeptieren.
7. Wählen Sie im Bereich **Gerätetypen, die Benutzer aktivieren können** die Gerätetypen iOS und Android aus.

8. Klicken Sie auf die Registerkarte **iOS** oder **Android**, und führen Sie die folgenden Schritte aus:
 - Wählen Sie in der Dropdown-Liste **Gerätmodell-Einschränkungen** aus, ob nur spezifische Geräte oder alle Gerätetypen zugelassen sind. Wenn Sie eine andere Option als **Keine Beschränkung** auswählen, klicken Sie auf **Bearbeiten**, wählen Sie die Geräte, die Sie sperren oder zulassen möchten, und klicken Sie dann auf **Speichern**.
 - Wählen Sie in der Dropdown-Liste **Zugelassene Version** die Version aus, die als Mindestanforderung zugelassen ist.
 - Wählen Sie im Abschnitt **Aktivierungsart** die Option **Geräteregistrierung nur für BlackBerry 2FA** aus.
9. Klicken Sie auf **Hinzufügen**.

Zuweisen eines Aktivierungsprofils nur für die Registrierung für Benutzer mit nicht verwalteten Geräten

Führen Sie die folgenden Aufgaben aus, um Benutzern, deren Geräte nicht von BlackBerry UEM verwaltet werden, ein Profil zuzuweisen. Diese Geräte müssen über BlackBerry UEM registriert werden, damit sie in BlackBerry 2FA verwendet werden können. Diese Aktivierungsart ist nur für iOS- und Android-Geräte verfügbar.

Bevor Sie beginnen:

- [Erstellen eines Aktivierungsprofils für die Registrierung von nicht verwalteten Geräten in BlackBerry 2FA.](#)
1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Benutzer**.
 2. Suchen Sie nach einem Benutzer.
 3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzers.
 4. Klicken Sie im Abschnitt **IT-Richtlinien und -Profile** auf **+**.
 5. Klicken Sie auf **Aktivierung**.
 6. Klicken Sie in der Dropdown-Liste **Aktivierungsprofil** auf das Aktivierungsprofil, das Sie erstellt haben, um die Registrierung nicht verwalteter Geräte zu Verwendung von BlackBerry 2FA zuzulassen.
 7. Wenn das in Schritt 6 ausgewählte Profil dem Benutzer bereits direkt zugewiesen ist, klicken Sie auf **Ersetzen**. Klicken Sie andernfalls auf **Zuweisen**.

Aktivieren eines BlackBerry 10-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Navigieren Sie auf dem Gerät zu **Einstellungen**.
2. Tippen Sie auf **Konten**.
3. Wenn Sie auf diesem Gerät über vorhandene Konten verfügen, tippen Sie auf **Konto hinzufügen**. Andernfalls fahren Sie mit Schritt 4 fort.
4. Tippen Sie auf **E-Mail, Kalender und Kontakte**.
5. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Weiter**.
6. Geben Sie im Feld **Kenntwort** das empfangene Aktivierungskennwort ein. Tippen Sie auf **Weiter**.
7. Wenn Sie anhand einer Warnmeldung informiert werden, dass Ihr Gerät die Verbindungsinformationen nicht finden konnte, führen Sie die folgenden Schritte aus:
 - a) Tippen Sie auf **Erweitert**.
 - b) Tippen Sie auf **Geschäftliches Konto**.

- c) Geben Sie im Feld **Serveradresse** die Adresse des Servers ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail, die Ihnen zugesendet wurde, oder im BlackBerry UEM Self-Service.
- d) Tippen Sie auf **Fertig**.

8. Folgen Sie den Anweisungen auf dem Bildschirm, um den Aktivierungsprozess abzuschließen.

Wenn Sie fertig sind: Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Navigieren Sie auf dem Gerät zum BlackBerry Hub, und bestätigen Sie, dass die E-Mail-Adresse vorhanden ist. Navigieren Sie zum Kalender, und bestätigen Sie, dass die Kalendertermine vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.
- Überprüfen Sie im Arbeitsbereich der Benutzer, ob die BlackBerry 2FA-App auf das Gerät des Benutzers heruntergeladen und installiert wurde. Wenn dies nicht der Fall ist, kann die BlackBerry 2FA-App von BlackBerry World für den geschäftlichen Bereich heruntergeladen werden.

Aktivieren eines iOS-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Installieren Sie den BlackBerry UEM Client auf dem Gerät. Kann aus dem Apple App Store heruntergeladen werden.
2. Tippen Sie auf dem Gerät auf **BlackBerry UEM**.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf **Ich stimme zu**.
4. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Go**.
5. Geben Sie ggf. die Serveradresse ein, und tippen Sie auf **Go**. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail, die Ihnen zugesendet wurde, oder im BlackBerry UEM Self-Service.
6. Bestätigen Sie, dass die auf dem Gerät angezeigten Zertifikatsdaten korrekt sind, und tippen Sie auf **Annehmen**. Falls Sie die Zertifikatsdaten von Ihrem Administrator separat erhalten haben, können Sie die angezeigten Informationen mit den Informationen vergleichen, die Sie erhalten haben.
7. Geben Sie Ihr Aktivierungskennwort ein, und tippen Sie auf **Mein Gerät aktivieren**.
8. Tippen Sie auf **OK**, um das erforderliche Zertifikat zu installieren.
9. Folgen Sie den Anweisungen auf dem Bildschirm, um die Aktivierung abzuschließen.
10. Wenn Sie aufgefordert werden, das Kennwort für Ihr E-Mail-Konto oder das Kennwort für Ihr Gerät einzugeben, folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie fertig sind: Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie den BlackBerry UEM Client auf dem Gerät, und tippen Sie auf **Info**. Überprüfen Sie im Abschnitt **Aktiviertes Gerät** und **Kompatibilitätsstatus**, ob die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivieren eines Android-Geräts

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Installieren Sie den BlackBerry UEM Client auf dem Gerät. Sie können den BlackBerry UEM Client aus dem Google Play herunterladen.
2. Tippen Sie auf dem Gerät auf **BlackBerry UEM**.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf **Ich stimme zu**.
4. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Weiter**.
5. Geben Sie ggf. die Serveradresse ein, und tippen Sie auf **Weiter**. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail, die Ihnen zugesendet wurde, oder im BlackBerry UEM Self-Service.
6. Bestätigen Sie, dass die auf dem Gerät angezeigten Zertifikatsdaten korrekt sind, und tippen Sie auf **Annehmen**. Falls Sie die Zertifikatsdaten von Ihrem Administrator separat erhalten haben, können Sie die angezeigten Informationen mit den Informationen vergleichen, die Sie erhalten haben.
7. Geben Sie Ihr Aktivierungskennwort ein, und tippen Sie auf **Mein Gerät aktivieren**.
8. Tippen Sie auf **Weiter**.
9. Tippen Sie auf **Aktivieren**.

Wenn Sie fertig sind: Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie den BlackBerry UEM Client auf dem Gerät, und tippen Sie auf **Info**. Überprüfen Sie im Abschnitt für das **aktivierte Gerät**, dass die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Einrichten oder Zurücksetzen einer Vorauthentifizierung

Führen Sie die folgende Aufgabe aus, wenn die BlackBerry 2FA-Vorauthentifizierung in Ihrem Unternehmen über Anfragen für IT-Dienste verwaltet wird, oder wenn Sie bestehende Einstellungen für die Vorauthentifizierung für einen Benutzer ändern möchten.

Bevor Sie beginnen:

- Stellen Sie sicher, dass dem Benutzer ein BlackBerry 2FA-Profil zugewiesen ist.
1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Benutzer**.
 2. Suchen Sie nach einem Benutzer.
 3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzers.
 4. In der Zusammenfassung klicken Sie auf **BlackBerry 2FA-Umgehung aktivieren**
 5. Geben Sie im Dialogfeld **Umgehungszeitraum festlegen** an, für wie viele Stunden Benutzer auf die Ressourcen Ihres Unternehmens Zugriff haben dürfen, ohne auf eine Bestätigungsaufforderung auf ihren Geräten antworten oder ein Einmalkennwort von einem Token senden zu müssen.
 6. Klicken Sie auf **Speichern**. Die Dauer wird in der Benutzerzusammenfassung angezeigt.
 7. Klicken Sie in der Benutzerzusammenfassung optional auf **Abbrechen**, um den Vorauthentifizierungszeitraum zu beenden. Benutzer können den Vorauthentifizierungszeitraum auch über **Läuft jetzt ab** in BlackBerry UEM Self-Service beenden.

Schritte für die Verwaltung von OTP-Hardware-Token

Führen Sie die folgenden Schritte zur Verwendung der Einmalkennwort-Tokenfunktion (OTP) aus:

Schritt	Aktion
1	Aktivieren der OTP-Tokenfunktion.
2	Konvertieren Sie bei Bedarf eine Token-Informationsdatei von einer XML-Datei in das PSKC-Format und schließlich in eine CSV-Datei, die Sie in BlackBerry UEM, Verwenden des BlackBerry 2FA Token Conversion Tool importieren können. Weitere Informationen finden Sie unter Bearbeiten der CSVConfig-Konfigurationsdatei .
3	Importieren von OTP-Token in BlackBerry UEM
4	Zuweisen eines OTP-Token zu einem Benutzer

Aktivieren der OTP-Tokenfunktion

1. Klicken Sie in der Menüleiste auf **Einstellungen** > **Externe Integration** > **Token für Einmalkennwort**.
2. Klicken Sie auf **Aktivieren**.
3. Klicken Sie auf **Aktivieren**.

Deaktivieren der OTP-Tokenfunktion

1. Klicken Sie in der Menüleiste auf **Einstellungen** > **Externe Integration** > **Token für Einmalkennwort**.
2. Klicken Sie auf **Verwaltung von Einmalkennwort-Token deaktivieren**.
3. Entfernen Sie die OTP-Token ggf. aus BlackBerry UEM. Weitere Informationen finden Sie unter [Entfernen eines OTP-Token aus BlackBerry UEM](#).

Unterstützte OTP-Hardware-Token

BlackBerry 2FA unterstützt derzeit die folgenden Einmalkennwort (OTP)-Hardware-Token von Drittanbietern:

- RCDevs RC200
- Vasco DIGIPASS GO 6
- Feitian OTP C200

In künftigen Versionen wird die Unterstützung weiterer Hardware-Token folgen. Die neuesten Informationen zur Kompatibilität von Hardware-Token finden Sie in der [Server-Kompatibilitätsmatrix](#).

Verwenden des BlackBerry 2FA Token Conversion Tool

Hinweis: Dieses Werkzeug ist nur für BlackBerry UEM 12.7 verfügbar und erforderlich. Für BlackBerry UEM 12.8 und höher und BlackBerry UEM Cloud können die Token-Informationsdateien ohne Verwendung des Tools direkt in UEM importiert werden.

Verwenden Sie das BlackBerry 2FA Token Conversion Tool, um eine Token-Informationsdatei von einer XML-Datei in das PSKC-Format und schließlich in eine CSV-Datei zu konvertieren, die Sie in BlackBerry UEM importieren können. Bei erfolgreicher Dateikonvertierung wird die generierte Datei automatisch in demselben Ordner abgelegt, in dem sich das Tool befindet.

Bei Vasco- und Feitian-Token müssen Sie das BlackBerry 2FA Token Conversion Tool verwenden, um die Token-Informationsdateien, die der Token-Hersteller bereitstellt, in ein Format zu konvertieren, die BlackBerry UEM lesen kann.

Das BlackBerry 2FA Token Conversion Tool unterstützt nur Token-Informationsdateien im PSKC-Format (Portable Symmetric Key Container). Weitere Informationen zu PSKCs finden Sie unter <https://tools.ietf.org/html/rfc6030>.

Wichtig: Die generierte Datei enthält Token-Informationen in nicht verschlüsselter Form. Es wird dringend empfohlen, dass Sie das BlackBerry 2FA Token Conversion Tool nur in einer sicheren Computerumgebung ausführen und die generierten Dateien nach dem Import in BlackBerry UEM umgehend löschen.

Bevor Sie beginnen:

- Laden Sie sich das BlackBerry 2FA Token Conversion Tool unter <https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B> herunter.
 - Legen Sie die Token-Informationsdateien, die Sie konvertieren möchten, in denselben Ordner, in dem sich das Tool befindet.
1. Öffnen Sie die Befehlszeile.
 2. Durchsuchen Sie das Verzeichnis des BlackBerry 2FA Token Conversion Tool.
 3. Führen Sie das **tokenConversionTool-<Version>.jar** mit den folgenden Parametern aus:

Parameter	Beschreibung
-h	Zum Anzeigen der Meldung zur Hilfenutzung.
-v	Optional, zum Aktivieren des ausführlichen Modus. Wenn Sie den ausführlichen Modus aktivieren, werden die Token-Informationsdateien in der festgelegten Datei in der Befehlszeile angezeigt.
-f	Geben Sie optional das Format an, in das die Konvertierung stattfinden soll („basic“ oder „rcdevs“). Der Standardwert ist „RCDevs“.
-p	Geben Sie bei Bedarf den Token-Schlüssel an, der erforderlich ist, um die Token-Informationsdatei zu entschlüsseln. Das Kennwort ist eine Folge von Byte im Hexadezimalformat (z. B. A12BC34D).
<i>filename</i>	Geben Sie die Datei an, die Sie konvertieren möchten. Die Datei muss sich im selben Ordner befinden wie das Tool. Dieser Parameter ist obligatorisch.

Geben Sie beispielsweise eine der folgenden Zeichenfolgen ein:

- `java -jar <ToolName>.jar -f basic -p <Kennwort> ./<TokenDateiName>.xml`
- `java -jar tokenConversionTool-1.0.4.jar ./vasco.xml`

Wenn die Datei erfolgreich generiert wurde, wird der Ausgabedateipfad angezeigt.

Wenn Sie fertig sind: Importieren Sie die generierte Token-Informationsdatei in die BlackBerry UEM-Verwaltungskonsole. Weitere Informationen finden Sie unter [Importieren von OTP-Token in BlackBerry UEM](#).

Bearbeiten der CSVConfig-Konfigurationsdatei

Die CSV-Datei mit den Tokendaten benötigt eine Konfigurationsdatei (CSVConfig.json), die definiert, wie die CSV-Datei von BlackBerry UEM analysiert werden soll. Eine korrekte Analyse der CSV-Datei ist vor dem Entpacken und Importieren der Tokendaten in die BlackBerry UEM-Datenbank erforderlich.

Wenn Sie sich zum ersten Mal nach dem Aktivieren der OTP-Tokenfunktion bei BlackBerry UEM anmelden, wird eine CSVConfig.json-Standarddatei generiert. Die Datei wird mit Standardwerten generiert und unter „BESNG_HOME“/otp/config/CSVConfig.json (oder C:\otp\config\CSVConfig.json) gespeichert.

Anhand der folgenden Informationen können Sie die CSVConfig.json-Datei so ändern, dass die CSV-Datei von BlackBerry UEM korrekt analysiert wird.

- Für „extension“ wird die Einstellung „CSV“ empfohlen.
- Die empfohlene Einstellung für „stripSpacesAndQuotations“ ist „true“. Alle Leerzeichen und Anführungszeichen aus den Spalten werden entfernt.
- Die Spalten für die entsprechenden Datenfelder können maximal vier Parameter aufweisen, die angeben, wie BlackBerry UEM die Daten aus der jeweiligen Spalte analysiert und extrahiert.
 - Der Wert für „column“ legt die Spaltennummer in der CSV-Datei fest. Spalten beginnen bei „0“.
 - Der Wert für „startCharPos“ gibt an, wo die Tokendaten in der Spalte beginnen. Wenn „stripSpacesAndQuotations“ auf „true“ gesetzt ist, werden nur die Zeichen vor dem Beginn der tatsächlichen Tokendaten und keine Leer- oder Anführungszeichen gezählt.
 - Der Wert für „endCharPos“ gibt an, wo die Tokendaten in der Spalte enden. Wenn „stripSpacesAndQuotations“ auf „true“ gesetzt ist, werden nur die Zeichen vor dem Ende der tatsächlichen Tokendaten und keine Leer- oder Anführungszeichen gezählt.
 - Der Wert für „encoding“ legt die verwendete Zeichenkodierung/-dekodierung fest. Als Standard wird „base64“ verwendet.

Im Folgenden finden Sie ein Beispiel einer CSVConfig.json-Datei, die für die Analyse einer CSV-Datei mit RCDevs-Tokendaten aktualisiert wurde:

```
{
  "extension" : "CSV",
  "stripSpacesAndQuotations" : true,
  "startRow" : 4,
  "token_serial_number" : {
    "column" : 1,
    "startCharPos" : 0
  },
  "password_seed" : {
    "column" : 3,
    "startCharPos" : 9,
    "encoding" : "base64"
  },
  "password_length" : {
```



```

    "column" : 6,
    "startCharPos" : 10,
    "encoding" : "base64"
  },
  "time_step" : {
    "column" : 7,
    "startCharPos" : 13,
    "encoding" : "base64"
  },
  "vendor" : {
    "column" : 2,
    "startCharPos" : 0,
    "endCharPos" : 6
  },
  "model" : {
    "column" : 2,
    "startCharPos" : 6,
    "endCharPos" : 14
  },
  "t0" : {
    "column" : 5,
    "startCharPos" : 11,
    "encoding" : "base64"
  }
}

```

Im Folgenden finden Sie ein Nur-Text-Beispiel einer CSV-Datei, die RCDevs-Tokendaten enthält:

```

1 # Inventory Import File for RCDevs WebADM
2 # Generated on June 29, 2016, 2:40 pm
3
4 Type                Reference                Description                Data
5 "OTP Token", "2308602200271", "RCDevs RC200-T6",
  "TokenKey=P6chCRszGaawHhpzWUHCS8Ua8WE=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
6 "OTP Token", "2308602200272", "RCDevs RC200-T6",
  "TokenKey=Zghe8fbekGOXpwGM2vmEcZyZnaE=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
7 "OTP Token", "2308602200273", "RCDevs RC200-T6",
  "TokenKey=EH//86f6pnup3F4AS7w7HNazYjU=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
8 "OTP Token", "2308602200274", "RCDevs RC200-T6", "TokenKey=tzrVqKFMns9/
  rbAyCYCdDxb04Ig=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
9 "OTP Token", "2308602200275", "RCDevs RC200-T6", "TokenKey=0FuZ/
  A6ZCVGClayW3EFcXWNFFk=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="

```

Importieren von OTP-Token in BlackBerry UEM



Zum Importieren von OTP-Token benötigen Sie eine CSV-Datei (Werte durch Kommata getrennt) mit den entsprechenden Token-Informationen. Die CSV-Datei wird von BlackBerry UEM mithilfe einer Konfigurationsdatei (CSVConfig.json) gelesen.

Bevor Sie beginnen: Sie müssen die CSVConfig.json-Standarddatei so anpassen, dass die Tokendaten von BlackBerry UEM korrekt analysiert und dann in der Datenbank gespeichert werden können. Weitere Informationen finden Sie unter [Bearbeiten der CSVConfig-Konfigurationsdatei](#).

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Token für Einmalkennwort**.
2. Klicken Sie auf **Durchsuchen**.
3. Wechseln Sie zu der CSV-Datei, die die Informationen zu den Token beinhaltet, und wählen Sie sie aus.

4. Klicken Sie auf **Hochladen**.

Entfernen eines OTP-Token aus BlackBerry UEM

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Token für Einmalkennwort**.
2. Suchen Sie nach der Seriennummer des zu entfernenden Token, und wählen Sie diese aus.
3.  Klicken Sie auf  .
4. Klicken Sie auf **Löschen**.

Zuweisen eines OTP-Token zu einem Benutzer

Bevor Sie beginnen: [Zuweisen eines BlackBerry 2FA-Profiles zu einem Benutzer](#).

1. Klicken Sie in der Menüleiste auf **Benutzer**. Suchen Sie nach dem Benutzernamen, und wählen Sie den Benutzer aus.
2. Klicken Sie auf der Seite mit den Detailinformationen auf **Einmalkennwort-Token**.
3. Suchen Sie nach der Seriennummer des Tokens, das Sie einem Benutzer zuweisen möchten, und wählen Sie diese aus.
4. Klicken Sie auf **Zuweisen**.

Entfernen eines OTP-Token von einem Benutzer

1. Klicken Sie in der Menüleiste auf **Benutzer**. Suchen Sie nach dem Benutzernamen, und wählen Sie den Benutzer aus.
2. Klicken Sie auf der Seite mit den Detailinformationen auf **Einmalkennwort-Token**.
3. Klicken Sie unter **Zugewiesene Token** auf **Entfernen**.
4. Klicken Sie auf **Anwenden**, um die Zuweisung des Einmalkennwort-Token aufzuheben.


Nicht synchronisierte Hardware-Token automatisch anpassen

Sie können das Zeitschrittfenster für Hardware-Token automatisch an die Token-Verschiebung anpassen. Wenn die interne Uhr des Hardware-Tokens zu stark von der korrekten Uhrzeit abweicht, zeigt das Token ungültige Codes an. Wenn Sie das Zeitschrittfenster vergrößern, ist jeder Code innerhalb dieses Fensters gültig, auch wenn das Token nicht synchronisiert ist.

Wenn Sie beispielsweise das Zeitschrittfenster auf "2" einstellen, wird der auf dem Token angezeigte Code als gültiger Code akzeptiert, wenn er dem erwarteten Code um zwei Aktualisierungsintervalle vorausgeht oder ihm folgt. Wenn in diesem Beispiel der auf dem Token angezeigte Code der dritte Code vor oder nach dem erwarteten Code ist, wird der Code als ungültig betrachtet und das Einmalpasswort wird abgelehnt.

Mit dieser Einstellung wird das Zeitschrittfenster für alle Hardware-Token angepasst. Stellen Sie das Zeitschrittfenster entsprechend der Anzahl der Aktualisierungsintervalle ein, in denen die Token Ihrer Meinung nach nicht synchronisiert sind.

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > Externe Integration**.
2. Klicken Sie auf **BlackBerry 2FA Token für Einmalkennwort**.

3. Klicken Sie im Feld **Zeitschrittfenster** auf .
4. Geben Sie einen Wert zwischen 0 und 50 ein. Der Standardwert ist 3. Um nur den erwarteten Code zu akzeptieren, der möglicherweise nicht mit dem auf dem Token angezeigten Code übereinstimmt, setzen Sie den Wert des Zeitschrittfensters auf 0.
5. Klicken Sie auf **Aktualisieren**.

Manuelles erneutes Synchronisieren eines Hardware-Tokens

Wenn ein Einmalkennwort-Hardware-Token, der einem Benutzer zugeordnet ist, nicht verwendbar ist, da die Verschiebung nicht automatisch angepasst wurde, können Sie versuchen, das Token manuell neu zu synchronisieren. Um ein Token manuell mit BlackBerry UEM neu zu synchronisieren, muss der Benutzer Ihnen zwei neue fortlaufende Codes geben.

1. Klicken Sie in der Menüleiste auf **Benutzer**. Suchen Sie nach dem Benutzernamen, und wählen Sie den Benutzer aus.
2. Klicken Sie auf **Token für Einmalkennwort**.
3. Klicken Sie im Abschnitt **Zugewiesene Token** auf **Erneut synchronisieren**.
4. Geben Sie im **Zeitschrittfenster** die maximale Anzahl der Zeitschritte ein, die Sie für das nicht synchronisierte Token erneut synchronisieren möchten.
5. Geben Sie den Code, der auf dem Token angezeigt wird, in das Feld **Erster Token-Code** ein.
6. Geben Sie den nächsten fortlaufenden Code, der auf dem Token angezeigt wird, in das Feld **Zweiter Token-Code** ein.
7. Klicken Sie auf **Erneut synchronisieren**.

Protokollierung und Reporting

BlackBerry UEM erzeugt Protokolle für die Vorauthentifizierungs- und Wiederherstellungsfunktionen in BlackBerry 2FA. Die Protokolle werden in der BlackBerry UEM Core (CORE)-Protokolldatei gespeichert.

Zusätzlich zu den Protokollinformationen, die für generelle Fehlerbehebungen nötig sind, erstellt BlackBerry UEM zu Prüfzwecken auch spezielle Protokollzeilen für die Vorauthentifizierung und die Wiederherstellung. Diese Protokollzeilen können extrahiert werden, um den allgemeinen Gebrauch der Vorauthentifizierungs- und Wiederherstellungsfunktionen zu überprüfen. Diese Protokollzeilen werden auf der INFO-Ebene protokolliert und bestehen aus durch Komma getrennte Daten, denen die universellen CORE-Protokollinformationen vorangestellt sind. Diese können verworfen werden.

Diese speziellen Protokollzeilen sind optisch hervorgehoben, damit sie leichter extrahiert werden können. Zwei Aktivitäten werden überwacht: Vorauthentifizierungsanfragen und Authentifizierungsanfragen während der Vorauthentifizierungsphase. Wenn diese Zeilen extrahiert und die CORE-Protokollinformationen verworfen wurden, können die durch Komma getrennten Daten mit einer beliebigen Software, die das CSV-Format unterstützt, geöffnet werden. Weitere Informationen zur Protokollierung und zum Reporting finden Sie in der Dokumentation zur [BlackBerry UEM Wartung und Überwachung](#).

Überwachung von Vorauthentifizierungsanfragen

BlackBerry UEM protokolliert jede BlackBerry 2FA-Vorauthentifizierungsanfrage und jede Authentifizierungsanfrage in der Vorauthentifizierungsphase. Die Daten werden protokolliert, wenn die Anfrage abgeschlossen wird oder abläuft.

Die Überwachungsprotokolldatei enthält die folgenden Informationen zu jeder Vorauthentifizierungsanfrage:

- Marker1: BB2FA_AUDIT. Das ist die Kennung für alle BlackBerry 2FA-Überwachungsprotokollzeilen im BlackBerry UEM Core-Protokoll. Dies zeigt außerdem an, wo die Protokollzeilen gekürzt werden müssen, um universelle CORE-Protokollinformationen zu verwerfen.
- Marker2: PREAUTH_REQUEST. Das ist die Kennung für den Ereignistyp (Vorauthentifizierungsanfrage).
- Datum
- Uhrzeit
- Quelle: BlackBerry UEM-Verwaltungskonsole, BlackBerry UEM Self-Service, Benutzergerät
- Benutzername
- BlackBerry 2FA-Profilname: Der Name wird in Anführungszeichen protokolliert, um die Aufteilung des Felds durch Kommas im Profil zu vermeiden.
- Dauer der Vorauthentifizierungsanfrage in Stunden
- Konfigurierte maximale Dauer der Vorauthentifizierungsanfrage in Stunden
- Ergebnis: SUCCESS, FAILED_INVALID_REQUEST
- Ablaufzeit der Vorauthentifizierungsanfrage

Beispiel:

```
2BB2FA_AUDIT,PREAUTH_REQUEST,2016-11-05,13:27:17.822,admin,user1,"Sales BB2FA Profile",3,12,May 11 16:41
```

In der Überwachungsprotokolldatei werden für jede Anfrage die folgenden Informationen in der Vorauthentifizierungsphase eingetragen:

- Marker1: BB2FA_AUDIT. Das ist die Kennung für alle BlackBerry 2FA-Überwachungsprotokollzeilen im BlackBerry UEM Core-Protokoll. Dies zeigt außerdem an, wo die Protokollzeilen gekürzt werden müssen, um universelle CORE-Protokollinformationen zu verwerfen.

- Marker2: AUTH_USER_IN_PREAUTH. Das ist die Kennung für den Ereignistyp (Authentifizierungsanfrage in der Vorauthentifizierungsphase).
- Datum
- Uhrzeit
- Transaktion-ID
- Quelle: BlackBerry 2FA-App, BlackBerry Enterprise Identity usw.
- Benutzername
- Authentifizierungsrichtlinien: Enterprise-Kennwort, Kennwort für das aktive Gerät, Kennwort für das passive Gerät
- Profilname: Der Name wird in Anführungszeichen protokolliert, um die Aufteilung des Felds durch Kommas im Profil zu vermeiden.
- Ablaufzeit der Vorauthentifizierungsanfrage

Beispiel:

```
BB2FA_AUDIT,AUTH_USER_IN_PREAUTH,2016-11-05,13:27:17.822,50dbelcc,BB2FA,user1,Enterprise Password,"Sales BB2FA Profile",May 11 16:41
```

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.

Android ist eine Marke von Google Inc. 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. Microsoft und Windows sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. 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.

SO FERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIE, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, BEDINGUNGEN, BILLIGUNGEN, GARANTIE, 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, USANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDE 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, SO FERN 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, 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 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 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 DARGELEGTE 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