



BlackBerry UEM Cloud

Architektur und -Datenflüsse

Inhalt

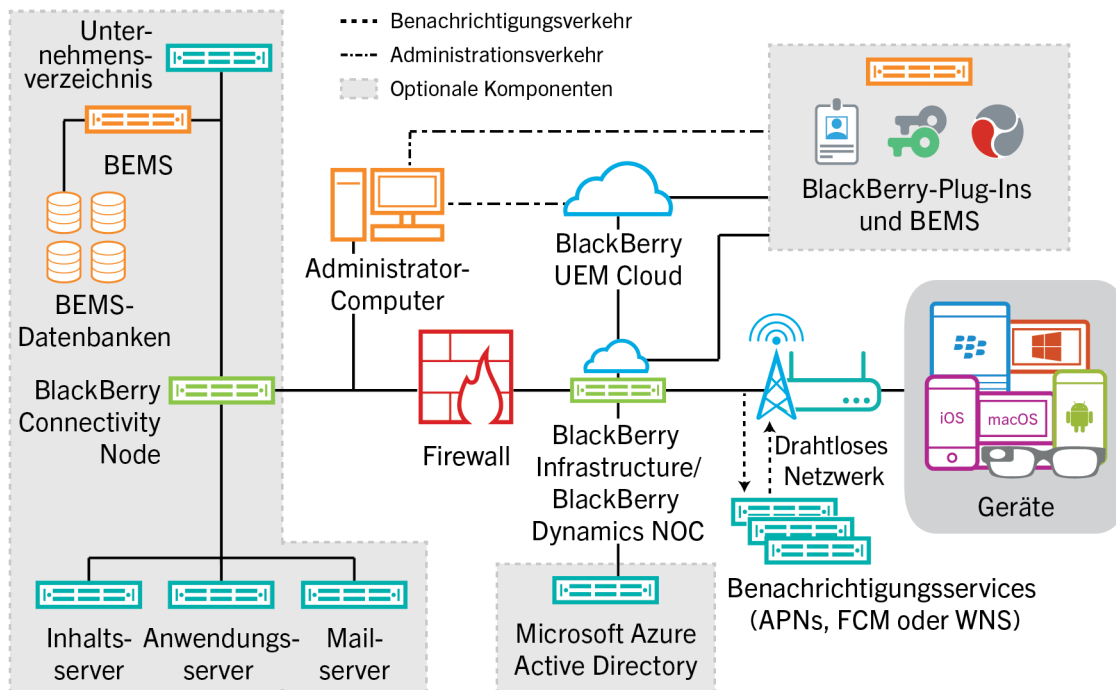
| | |
|--|-----------|
| BlackBerry UEM Cloud-Architektur und Datenstrom..... | 4 |
| Architektur: BlackBerry UEM Cloud-Lösung..... | 4 |
| Aktivieren von Geräten und BlackBerry Dynamics-Apps..... | 8 |
| Datenfluss: Aktivieren eines Geräts mit iOS, Android oder Windows 10..... | 8 |
| Datenfluss: Aktivieren eines macOS-Geräts..... | 10 |
| Datenfluss: Erstmaliges Aktivieren einer BlackBerry Dynamics-App auf einem Gerät..... | 11 |
| Datenfluss: Aktivieren einer -BlackBerry Dynamics-App, wenn bereits eine App auf dem Gerät aktiviert ist..... | 12 |
| Datenfluss: Empfangen von Konfigurationsupdates auf einem Gerät..... | 13 |
| Senden und Empfangen von geschäftlichen Daten..... | 15 |
| Senden und Empfangen von geschäftlichen Daten über BlackBerry UEM Cloud und die BlackBerry Infrastructure..... | 17 |
| Datenfluss: Senden einer E-Mail von einem iOS-Gerät mithilfe des BlackBerry Secure Gateway..... | 18 |
| Datenfluss: Empfangen einer E-Mail auf einem iOS-Gerät mithilfe von BlackBerry Secure Gateway..... | 18 |
| Datenfluss: Senden und Empfangen von geschäftlichen Daten mit BlackBerry Secure Connect Plus..... | 19 |
| Datenfluss: Senden und Empfangen von geschäftlichen Daten von einer BlackBerry Dynamics-App auf einem Android-Gerät unter Verwendung von BlackBerry Secure Connect Plus..... | 20 |
| Datenfluss: Senden und Empfangen von geschäftlichen Daten von einer BlackBerry Dynamics-App..... | 21 |
| Datenfluss: Senden und Empfangen von geschäftlichen Daten von einer BlackBerry Dynamics-App unter Verwendung von BlackBerry Dynamics Direct Connect..... | 21 |
| Senden und Empfangen von geschäftlichen Daten über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk... | 23 |
| Datenfluss: Senden einer E-Mail von einem Gerät über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk..... | 23 |
| Datenfluss: Empfangen einer E-Mail auf einem Gerät über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk..... | 24 |
| Datenfluss: Zugreifen auf einen Anwendungs- oder Inhaltsserver über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk..... | 25 |
| Rechtliche Hinweise..... | 26 |

BlackBerry UEM Cloud-Architektur und Datenstrom

BlackBerry UEM Cloud ist eine einheitliche Lösung zur Endpunktverwaltung von BlackBerry. Mit BlackBerry UEM Cloud können Sie iOS-, macOS-, Android- und Windows 10-Geräte über eine einfache webbasierte Oberfläche verwalten und geschäftliche Daten auf BYOD-, COPE- und COBO-Geräten schützen.

Die BlackBerry UEM Cloud-Architektur wurde entwickelt, um Sie bei der Verwaltung mobiler Geräte für Ihr Unternehmen in einer Cloud-Umgebung zu unterstützen und eine sichere Verbindung für Daten bereitzustellen, die zwischen E-Mail- und Inhaltsservern und den Geräten der Benutzer übertragen werden.

Architektur: BlackBerry UEM Cloud-Lösung



| Komponente | Beschreibung |
|---|--|
| BlackBerry UEM Cloud | BlackBerry UEM Cloud ist ein Dienst für die Verwaltung von Geräten, die in der Umgebung Ihres Unternehmens verwendet werden. |
| BlackBerry Infrastructure und BlackBerry Dynamics NOC | Die BlackBerry Infrastructure registriert Benutzerinformationen für die Geräteaktivierung und überprüft Lizenzinformationen für BlackBerry UEM Cloud. Wenn Sie BlackBerry Secure Connect Plus oder BlackBerry Secure Gateway aktivieren, werden Daten, die diese Dienste verwenden, bei der Übertragung über die BlackBerry Infrastructure geleitet. BlackBerry Dynamics NOC ist ein separates Netzbetriebszentrum (Network Operation Center, NOC), das eine sichere Kommunikation zwischen BlackBerry Dynamics-Apps auf Geräten und BlackBerry Proxy hinter der Firewall als Teil des BlackBerry Connectivity Node bietet. |

| Komponente | Beschreibung |
|--------------------------|---|
| Geräte | BlackBerry UEM Cloud unterstützt Geräte mit iOS, macOS, Android und Windows 10. |
| Benachrichtigungsdienste | <p>BlackBerry UEM Cloud sendet Benachrichtigungen an Geräte, um mögliche Updates von BlackBerry UEM abzurufen und Informationen über den Gerätebestand Ihres Unternehmens zu übermitteln. Diese Benachrichtigungen werden an die BlackBerry Infrastructure gesendet, wo sie mithilfe des entsprechenden Benachrichtigungsdiensts an die Geräte gesendet werden.</p> <ul style="list-style-type: none"> • APNs ist ein Apple-Dienst zum Senden von Benachrichtigungen an iOS- und macOS-Geräte. • FCM ist ein Google-Dienst zum Senden von Benachrichtigungen an Android-Geräte. • WNS ist ein Microsoft-Dienst zum Senden von Benachrichtigungen an Windows 10-Geräte. |

| Komponente | Beschreibung |
|------------------------------|--|
| BlackBerry Connectivity Node | <p>Der BlackBerry Connectivity Node ist eine optionale Komponente, die Sie innerhalb der Firewall Ihres Unternehmens installieren. Er enthält fünf Komponenten, die BlackBerry UEM Cloud um weitere Funktionen erweitern:</p> <ul style="list-style-type: none"> • Der BlackBerry Cloud Connector stellt eine Verbindung zwischen Ihrem Unternehmensverzeichnis und BlackBerry UEM Cloud hinter der Firewall Ihres Unternehmens her, um die Synchronisierung von Attributen, eine Suchfunktion und Dienste zur Authentifizierung von Benutzern zuzulassen. Wenn Sie den BlackBerry Connectivity Node nicht installieren und sich Ihr Unternehmensverzeichnis hinter der Firewall befindet, müssen Sie lokale Benutzerkonten in BlackBerry UEM Cloud erstellen, anstatt die in Ihrem Unternehmensverzeichnis aufgeführten Benutzerkonten zu verwenden. Der BlackBerry Cloud Connector ist nicht erforderlich, damit BlackBerry UEM Cloud eine Verbindung zu Microsoft Azure Active Directory herstellt. • BlackBerry Proxy hält eine sichere Verbindung zwischen Ihrem Unternehmen und BlackBerry Dynamics NOC aufrecht, die BlackBerry Dynamics-Apps eine sichere Kommunikation mit den Ressourcen Ihres Unternehmens hinter der Firewall erlaubt. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen von BlackBerry Dynamics NOC ermöglicht. • Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf BlackBerry UEM Cloud aktiviert werden. Nicht verwaltete Geräte, die versuchen, sich mit einem E-Mail-Server des Unternehmens zu verbinden, können durch einen Administrator über die BlackBerry UEM-Verwaltungskonsole überprüft, verifiziert und blockiert oder zugelassen werden. • BlackBerry Secure Connect Plus stellt einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf Geräten und dem Netzwerk des Unternehmens her. Ein Tunnel, der standardmäßige IPV4-Daten (TCP und UDP) unterstützt, wird für jedes Gerät über die BlackBerry Infrastructure bereitgestellt. • Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM Cloud zum E-Mail-Server Ihres Unternehmens für iOS-Geräte. <p>Der BlackBerry Connectivity Node nutzt für die Kommunikation mit der BlackBerry UEM Cloud Port 3101.</p> |

| Komponente | Beschreibung |
|---|--|
| BlackBerry Enterprise Mobility Server | <p>Wenn Sie BlackBerry Connectivity Node installiert haben, ist auch eine Installation eines lokalen BEMS möglich. Der BEMS führt verschiedene Dienste zusammen, die zum Übertragen von geschäftlichen Daten zwischen BlackBerry Dynamics-Apps verwendet werden:</p> <ul style="list-style-type: none"> • BlackBerry Connect ermöglicht sicheres Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen auf iOS- und Android-Geräten. • BlackBerry Presence stellt Informationen zum Anwesenheitsstatus für BlackBerry Dynamics-Apps in Echtzeit bereit. • BlackBerry Docs ermöglicht den Benutzern der BlackBerry Dynamics-App den Zugriff, die Synchronisierung und die gemeinsame Nutzung von Dokumenten über ihren geschäftlichen Dateiserver, SharePoint, Box und Content-Management-Systeme mit CMIS-Unterstützung, ohne Einsatz von VPN-Software, ohne Firewall-Neukonfiguration oder doppelte Datenspeicher. |
| BlackBerry Enterprise Mobility Server-Datenbanken | In den BEMS-Datenbanken werden Benutzer-, App-, Richtlinien- und Konfigurationsinformationen gespeichert. |
| Unternehmensverzeichnis | BlackBerry UEM Cloud unterstützt Verbindungen zum Microsoft Active Directory Ihres Unternehmens bzw. zum LDAP-Unternehmensverzeichnis hinter der Firewall über den BlackBerry Connectivity Node. |
| Microsoft Azure Active Directory | Microsoft Azure Active Directory ist ein Cloud-basierter Verzeichnisverwaltungsdienst. Wenn Ihr Unternehmen Azure Active Directory verwendet, können Sie eine Verbindung dazu anstatt oder zusätzlich zum Unternehmensverzeichnis hinter der Firewall herstellen. |
| Inhalts-, Anwendungs- und Mail-Server | <p>Wenn Sie BlackBerry Secure Connect Plus aktivieren, oder wenn Benutzer BlackBerry Dynamics-Apps haben, können Geräte eine Verbindung mit den Servern Ihres Unternehmens herstellen, ohne dass Sie eine direkte Verbindung zwischen dem Server und dem Internet herstellen müssen. Geschäftliche Daten während der Übertragung zwischen Ihren Servern und Geräten werden über BlackBerry Secure Connect Plus und BlackBerry Infrastructure gesendet. BlackBerry Dynamics-App-Daten werden über BlackBerry Proxy und BlackBerry Dynamics NOC gesendet.</p> <p>BlackBerry Secure Gateway bietet eine sichere Verbindung über BlackBerry Infrastructure und BlackBerry Connectivity Node zwischen dem E-Mail-Server Ihres Unternehmens und iOS-Geräten.</p> |
| BlackBerry-Plug-ins und BEMS | <p>Die Cloud-Version von BlackBerry Enterprise Mobility Server stellt BlackBerry Push Notifications bereit und akzeptiert Push-Registrierungsanforderungen von iOS- und Android-Geräten und kommuniziert mit Microsoft Exchange, um das geschäftliche E-Mail-Konto des Benutzers auf Änderungen zu überwachen. Wenn Microsoft Exchange sich hinter der Firewall Ihres Unternehmens befindet, müssen Sie einen Port für BEMS öffnen, um mit Microsoft Exchange zu kommunizieren.</p> <p>BlackBerry UEM Cloud ist mit zusätzlichen BlackBerry-Unternehmensprodukten, z. B. BlackBerry Enterprise Identity, BlackBerry 2FA und BlackBerry Workspaces, kompatibel, um Ihnen die Erweiterung von UEM-Funktionen in Ihrem Unternehmen zu ermöglichen.</p> |

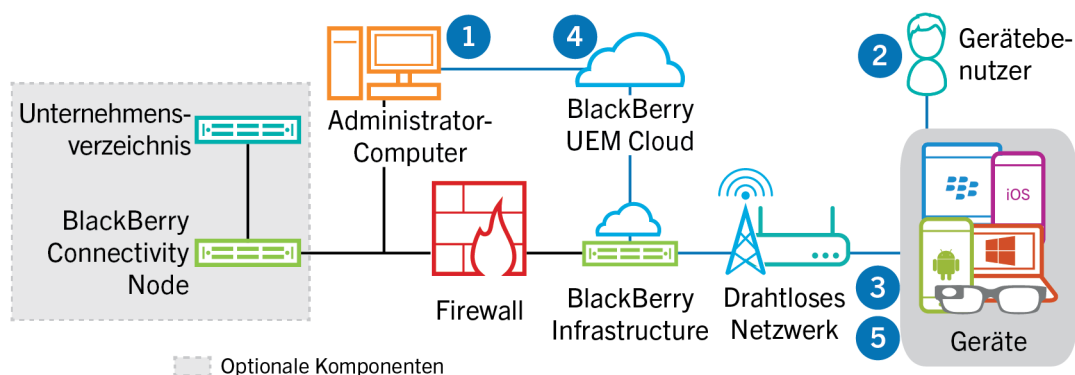
Aktivieren von Geräten und BlackBerry Dynamics-Apps

Wenn ein Benutzer ein Gerät mit BlackBerry UEM aktiviert, wird das Gerät mit BlackBerry UEM verknüpft, damit Sie das Gerät verwalten und Benutzer auf ihren Geräten auf geschäftliche Daten zugreifen können. Durch die Geräteaktivierungsarten haben Sie einen unterschiedlich hohen Einfluss auf die geschäftlichen und privaten Daten auf den Geräten: von der kompletten Kontrolle aller Daten bis hin zur Beschränkung der Kontrolle auf die geschäftlichen Daten. Weitere Informationen zu Aktivierungsarten finden Sie in der [Dokumentation für Administratoren unter „Geräteaktivierung“](#).

Je nach Gerätetyp und Aktivierungsart, die Sie für das Gerät angeben, müssen das Gerät und BlackBerry UEM mehrere Schritte während des Aktivierungsprozesses durchführen, um sich gegenseitig zu authentifizieren und einen Kommunikationskanal zu sichern. Sie erstellen bei Bedarf einen geschäftlichen Bereich oder verschlüsseln das Gerät, bevor Konfigurations- und geschäftliche Daten an Ihr Gerät gesendet werden. Anweisungen zum Aktivieren von Geräten finden Sie in der [Dokumentation für Administratoren unter „Schritte zum Aktivieren von Geräten“](#).

BlackBerry Dynamics-Apps bieten Zugriff auf geschäftliche Ressourcen auf dem Gerät. Nachdem BlackBerry Dynamics-Apps auf einem Gerät installiert wurden, müssen sie noch aktiviert werden, damit sie sicher auf Ihre geschäftlichen Ressourcen zugreifen können. Weitere Informationen zur Aktivierung von BlackBerry Dynamics finden Sie unter [„Erstellen von Zugriffsschlüsseln, Aktivierungskennwörtern oder QR Codes für BlackBerry Dynamics-Apps“](#) in der [Dokumentation für Administratoren](#).

Datenfluss: Aktivieren eines Geräts mit iOS, Android oder Windows 10

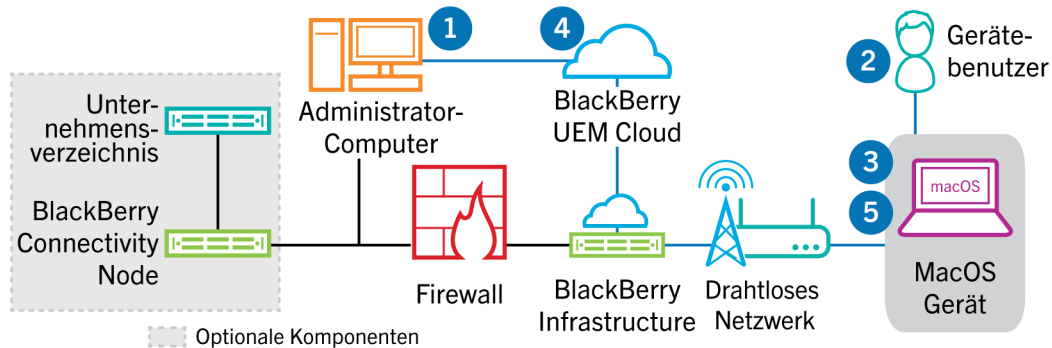


1. Führen Sie die folgenden Schritte aus:

- a. Fügen Sie einen Benutzer zu BlackBerry UEM Cloud als lokales Benutzerkonto oder, falls BlackBerry Connectivity Node installiert wurde, unter Verwendung von Kontoinformationen hinzu, die aus dem Unternehmensverzeichnis abgerufen werden.
- b. Weisen Sie dem Benutzer ein Aktivierungsprofil zu.
- c. Je nach Gerätetyp und den Präferenzen Ihrer Organisation, verwenden Sie eine der folgenden Optionen, um den Benutzern Benutzerdaten bereitzustellen:
 - Automatisches Generieren eines Geräteaktivierungskennworts und optional eines QR-Codes sowie das Senden einer E-Mail-Nachricht mit Aktivierungsanweisungen für den Benutzer
 - Einrichten eines Geräteaktivierungskennworts und Mitteilen des Benutzernamens und Kennworts an den Benutzer direkt oder per E-Mail
 - Kein Einrichten eines Geräteaktivierungskennworts und keine Mitteilung der BlackBerry UEM Self-Service-Adresse an den Benutzer, sodass der Benutzer ein eigenes Aktivierungskennwort festlegen oder einen QR-Code anzeigen kann

2. Der Benutzer führt die folgenden Aktionen aus:
 - a. Der Benutzer lädt bei der Aktivierung eines iOS- oder Android-Geräts den BlackBerry UEM Client herunter und installiert ihn.
 - b. Gibt Benutzernamen und Kennwort für die Aktivierung ein oder scannt den QR-Code auf Ihrem Gerät.
3. Das Gerät sendet eine Aktivierungsanforderung an BlackBerry UEM.
4. BlackBerry UEM Cloud überprüft die Anmeldeinformationen des Benutzers für die Aktivierung und sendet die Aktivierungsdetails an das Gerät, einschließlich der Gerätekonfigurationsinformationen.
5. Das Gerät empfängt die Aktivierungsdetails von BlackBerry UEM Cloud und schließt die Konfiguration ab. Das Gerät sendet dann die Bestätigung an BlackBerry UEM Cloud, dass die Aktivierung erfolgreich war.

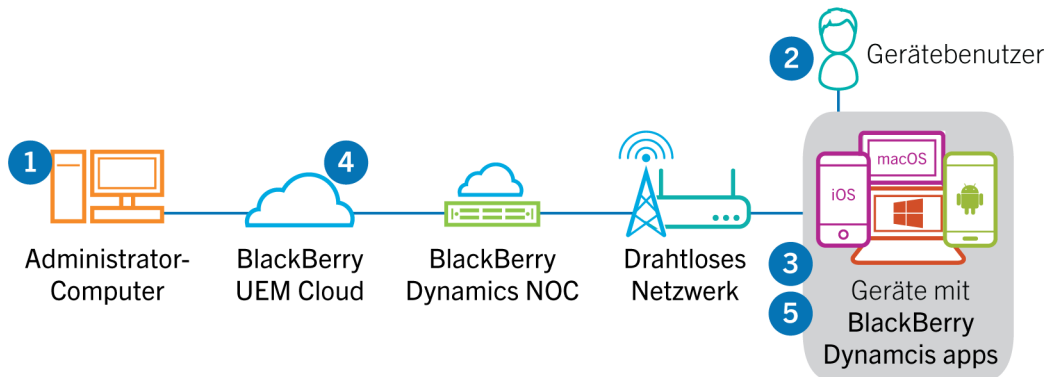
Datenfluss: Aktivieren eines macOS-Geräts



1. Führen Sie die folgenden Schritte aus:
 - a. Fügen Sie BlackBerry UEM Cloud den Benutzer als lokales Benutzerkonto hinzu oder, falls der BlackBerry Connectivity Node installiert ist, verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
 - b. Weisen Sie dem Benutzer ein Aktivierungsprofil zu.
 - c. Stellen Sie sicher, dass der Benutzer über die folgenden Anmeldeinformationen für BlackBerry UEM Self-Service verfügt:
 - Webadresse für BlackBerry UEM Self-Service
 - Benutzername und Kennwort
 - Domänenname
2. Der Benutzer meldet sich bei BlackBerry UEM Self-Service auf seinem macOS-Gerät an und aktiviert das Gerät.
3. Das Gerät sendet eine Aktivierungsanforderung an BlackBerry UEM Cloud.
4. BlackBerry UEM Cloud überprüft die Anmeldeinformationen für die Aktivierung und sendet die Aktivierungsdetails an das Gerät, einschließlich der Gerätekonfigurationsinformationen.
5. Das Gerät empfängt die Aktivierungsdetails von BlackBerry UEM Cloud und schließt die Konfiguration ab. Das Gerät sendet dann die Bestätigung an BlackBerry UEM Cloud, dass die Aktivierung erfolgreich war.

Datenfluss: Erstmaliges Aktivieren einer BlackBerry Dynamics-App auf einem Gerät

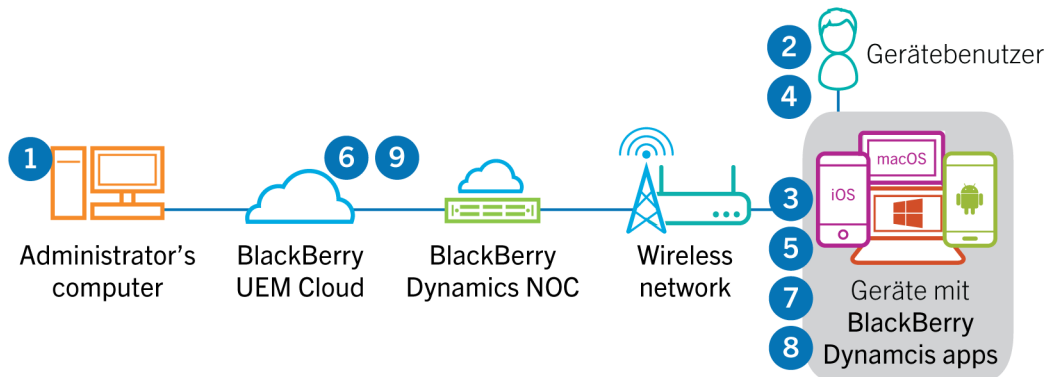
Dieser Datenfluss beschreibt, wie Daten übertragen werden, wenn eine BlackBerry Dynamics-App auf einem Gerät aktiviert wird und weder eine andere BlackBerry Dynamics-App noch der BlackBerry UEM Client bereits aktiviert ist.



1. Ein Administrator führt die folgenden Aktionen aus:
 - a. Er weist einem Benutzer BlackBerry Dynamics-Apps zu.
 - b. Er gibt Aktivierungszugangsdaten aus (Zugriffsschlüssel, Aktivierungskennwort oder QR Code) und sendet sie an den Benutzer oder weist den Benutzer an, Anmeldeinformationen aus BlackBerry UEM Self-Service zu generieren.
2. Der Benutzer führt die folgenden Aktionen aus:
 - a. Er installiert die App auf dem Gerät.
 - b. Er ruft die angegebenen Aktivierungszugangsdaten ab und gibt sie ein.
3. Die BlackBerry Dynamics-App führt die folgenden Aktionen aus:
 - a. Herstellen eine Verbindung zum BlackBerry Dynamics NOC und Abschließen der Aktivierung
 - b. Abrufen der BlackBerry UEM-Adresse mit einer der folgenden Methoden:
 - Wenn der Benutzer die Anmeldeinformationen manuell eingegeben hat, ruft die App die Adresse von der BlackBerry Infrastructure ab.
 - Wenn der Benutzer einen QR Code gescannt hat, erhält die App die Adresse vom QR Code.
 - c. Herstellen einer Verbindung mit BlackBerry UEM über die BlackBerry Infrastructure und Erstellen einer End-to-End-verschlüsselten Sitzung mit BlackBerry UEM mithilfe des EC-SPEKE-Protokolls
Diese Session kann nur von der BlackBerry UEM-Instanz entschlüsselt werden, die die Aktivierungsanmeldedaten ausgegeben hat.
 - d. Senden der Aktivierungsanforderung über die gesicherte Sitzung
4. BlackBerry UEM überprüft die Aktivierungsanforderung und sendet eine verschlüsselte Aktivierungsantwort an die App. Die Aktivierungsantwort enthält Daten, die von der App für die Kommunikation mit BlackBerry UEM benötigt werden, einschließlich Client-Zertifikat, Mastersessionschlüssel, Liste der BlackBerry Proxy-Instanzen und vertrauenswürdige Zertifizierungsstellen.
5. Die App fordert den Benutzer auf, ein Kennwort für die App festzulegen und diese als einfachen Aktivierungsdelegierten beim BlackBerry Dynamics NOC zu registrieren, damit die nachfolgende BlackBerry Dynamics-App auf dem Gerät aktiviert werden kann, ohne dass der Benutzer manuell neue Anmeldeinformationen erhält.

Datenfluss: Aktivieren einer -BlackBerry Dynamics-App, wenn bereits eine App auf dem Gerät aktiviert ist

Dieser Datenfluss beschreibt, wie Daten übertragen werden, wenn eine BlackBerry Dynamics-App auf einem Gerät aktiviert wird und der BlackBerry UEM Client oder eine andere BlackBerry Dynamics-App bereits aktiviert ist und als einfacher Aktivierungsdelegierter fungiert.



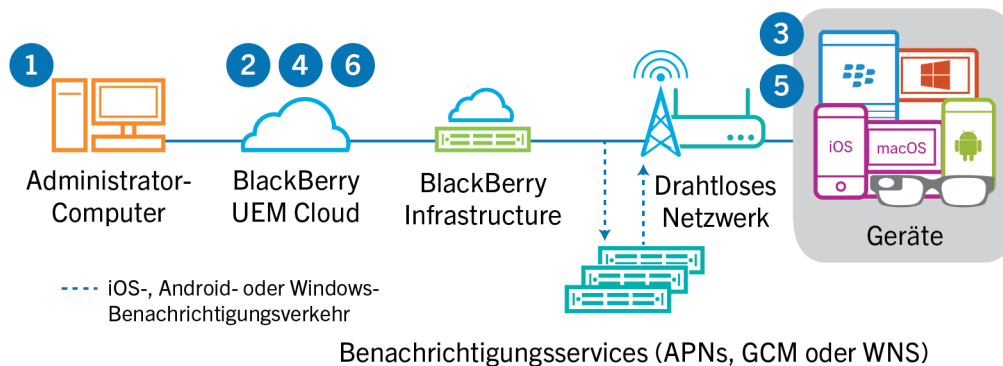
1. Ein Administrator weist einem Benutzer BlackBerry Dynamics-Apps zu.
2. Der Benutzer installiert die App auf seinem Gerät.
3. Die App führt die folgenden Aktionen aus:
 - a. Abfragen von BlackBerry Dynamics NOC und Identifizieren einer anderen App, die auf dem Gerät aktiviert ist
 - b. Anfordern der Aktivierungszugangsdaten von der zuvor aktivierten App
4. Der Benutzer genehmigt die Aktivierungsanforderung von der zuvor auf dem Gerät aktivierten App.
5. Die zuvor aktivierte App sendet die Anmeldeinformationen an BlackBerry UEM.
6. BlackBerry UEM sendet die Anmeldedatenanforderung und BlackBerry UEM-URL an die vorhandene App.
7. Die zuvor aktivierte App gibt die Anmeldeinformationen und die URL an die neue App zurück.
8. Die neue App führt die folgenden Aktionen aus:
 - a. Aktivierung mit BlackBerry Dynamics NOC
 - b. Herstellen einer Verbindung mit BlackBerry UEM über die BlackBerry Infrastructure und Erstellen einer End-to-End-verschlüsselten Sitzung mit BlackBerry UEM mithilfe des EC-SPEKE-Protokolls

Diese Session kann nur von der BlackBerry UEM-Instanz entschlüsselt werden, die die Aktivierungsanmeldedaten ausgegeben hat.
 - c. Senden der Aktivierungsanforderung über die gesicherte Sitzung
9. BlackBerry UEM überprüft die Aktivierungsanforderung und sendet eine verschlüsselte Aktivierungsantwort an die App. Die Aktivierungsantwort enthält Daten, die von der App für die Kommunikation mit BlackBerry UEM benötigt werden, einschließlich Client-Zertifikat, Mastersessionschlüssel, Liste der BlackBerry Proxy-Instanzen und vertrauenswürdige Zertifizierungsstellen.

Datenfluss: Empfangen von Konfigurationsupdates auf einem Gerät

Wenn Sie die Verwaltungskonsolle zum Senden von Gerätebefehlen verwenden, wie Gerät sperren oder geschäftliche Daten löschen, oder wenn Sie andere Geräteverwaltungsaufgaben ausführen (Aktualisierungen von IT-Richtlinien, Profilen und App-Einstellungen oder Zuweisungen), lösen Sie für das Gerät ein Konfigurationsupdate aus.

Muss ein Konfigurationsupdate an ein Gerät gesendet werden, benachrichtigt BlackBerry UEM Cloud die Geräte, dass ein Konfigurationsupdate aussteht. Geräte rufen von BlackBerry UEM Cloud regelmäßig Informationen zu Aktionen ab, die auf dem Gerät ausgeführt werden müssen, damit ein Konfigurationsupdate nicht verpasst wird, wenn eine Benachrichtigung nicht auf dem Gerät empfangen wird.



1. Sie verwenden die Verwaltungskonsolle, um Gerätebefehle zu senden, beispielsweise zum Sperren des Geräts oder zum Löschen von geschäftlichen Daten, oder Sie verwenden die Verwaltungskonsolle, um Verwaltungsaufgaben für Geräte durchzuführen, z. B. die Aktualisierung von IT-Richtlinien, Profilen, App-Einstellungen oder Zuweisungen, und lösen für das Gerät ein Konfigurationsupdate aus.
2. BlackBerry UEM Cloud weist das Update zu, ermittelt die Objekte, die für das Gerät freigegeben werden müssen, und führt dann folgende Aktionen aus:
 - Bei Android-Geräten benachrichtigt BlackBerry UEM Cloud den BlackBerry UEM Client auf dem Gerät mithilfe von FCM darüber, dass ein Update aussteht. FCM sendet eine Benachrichtigung an das Gerät mit der Aufforderung, Kontakt mit BlackBerry UEM Cloud aufzunehmen.
 - Bei iOS- und OS X-Geräten benachrichtigt BlackBerry UEM Cloud den MDM-Daemon auf dem Gerät mithilfe von APNs darüber, dass ein Update aussteht. APNs sendet eine Benachrichtigung an das Gerät mit der Aufforderung, Kontakt mit BlackBerry UEM Cloud aufzunehmen.
 - Bei Windows 10-Geräten benachrichtigt BlackBerry UEM Cloud den MDM-Daemon auf dem Gerät mithilfe von WNS darüber, dass ein Update aussteht. WNS sendet eine Benachrichtigung an das Gerät mit der Aufforderung, Kontakt mit BlackBerry UEM Cloud aufzunehmen.
3. Das Gerät nimmt Kontakt mit BlackBerry UEM Cloud auf, um ausstehende Aktionen anzufordern, die auf dem Gerät durchgeführt werden müssen.
4. BlackBerry UEM Cloud antwortet mit der höchsten Priorität.

IT-Administrationsbefehle wie das Sperren von Geräten werden vorrangig behandelt, gefolgt von Anforderungen für Geräteinformationen, installierte Apps usw. BlackBerry UEM Cloud sendet jeweils einen Befehl. Bei Bedarf enthält die Antwort zusätzliche Informationen.
5. Das Gerät führt die folgenden Aktionen aus:
 - a. Das Gerät prüft die Antwort von BlackBerry UEM Cloud
 - b. Das Gerät plant die Verarbeitung des Befehls und wartet auf den Befehl zur Durchführung

- c. Das Gerät sendet eine Antwort an BlackBerry UEM Cloud zur Aktualisierung des Befehlsstatus. Der Status zeigt an, ob der Befehl erfolgreich ausgeführt wurde, und gibt bei einem Fehler eine Fehlermeldung aus.
6. Wenn mehrere Aktionen oder Befehle für das Gerät ausstehen, antwortet BlackBerry UEM Cloud mit der höchsten Priorität.

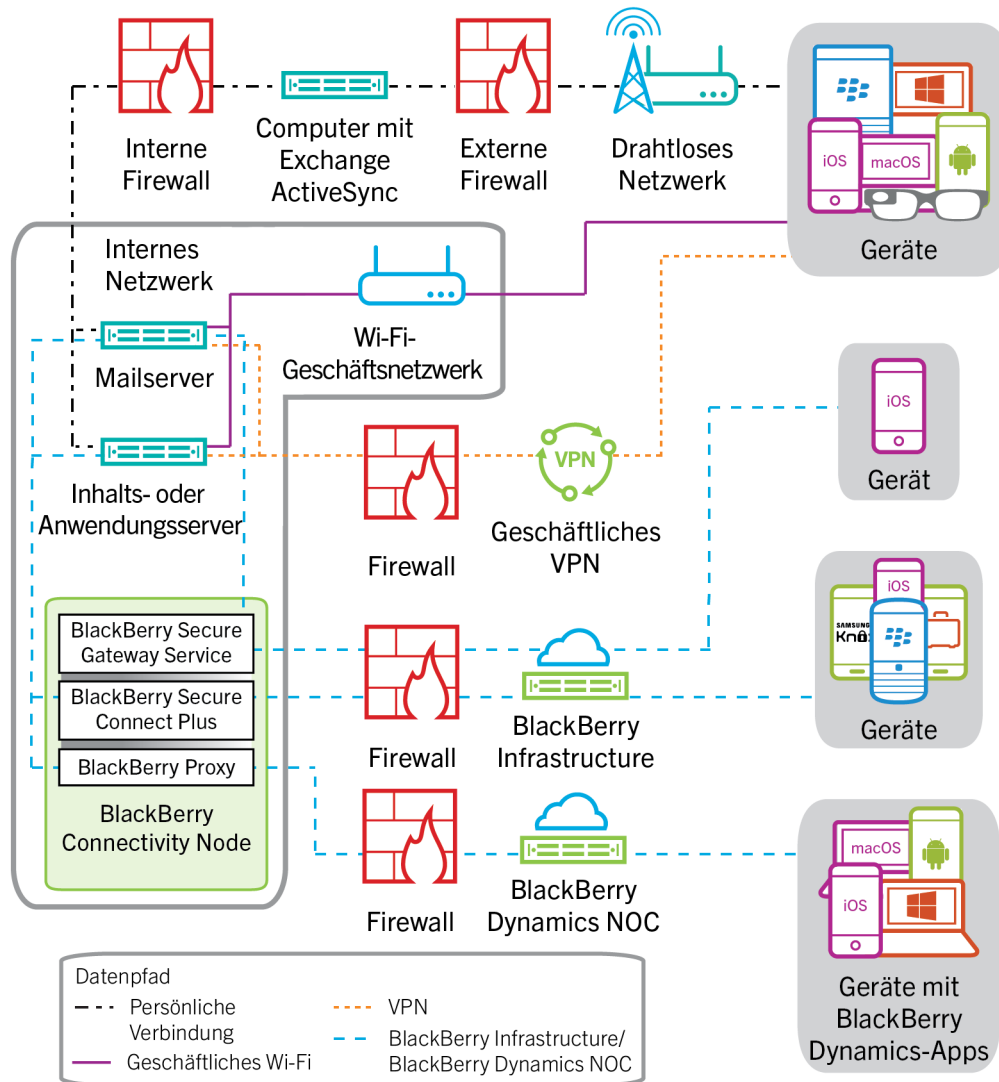
Schritte 4 bis 6 werden wiederholt, bis alle ausstehenden Aktionen oder Befehle auf dem Gerät durchgeführt wurden und BlackBerry UEM Cloud mit einem Leerlaufbefehl antwortet.

Senden und Empfangen von geschäftlichen Daten

Wenn Benutzer geschäftliche Daten auf einem Gerät senden und empfangen, können Daten zwischen dem Gerät und Ihren Ressourcen über die folgenden Verbindungen gesendet werden:

- Das Gerät kann eine direkte Verbindung über das mobile Netzwerk zwischen dem Gerät und einem Mail-, Inhalts- oder Anwendungsserver verwenden (z. B. einem Exchange ActiveSync-Server, der sich in einer DMZ oder in einem öffentlichen Netzwerk befindet).
- Das Gerät kann eine direkte Verbindung über das VPN Ihres Unternehmens oder das Wi-Fi-Geschäftsnetzwerk zum Mail-, Inhalts- oder Anwendungsserver verwenden. Das Geräte-VPN oder das Wi-Fi-Profil können von Ihnen oder den Benutzern konfiguriert werden.
- Wenn Sie den BlackBerry Connectivity Node installieren, kann BlackBerry Secure Connect Plus einen sicheren IP-Tunnel über die BlackBerry Infrastructure zwischen Apps auf iOS-, Android Enterprise- und Samsung Knox Workspace-Geräten und dem Netzwerk Ihres Unternehmens bereitstellen.
- Wenn Sie BlackBerry Connectivity Node installieren, kann BlackBerry Proxy eine sichere Verbindung zwischen BlackBerry Dynamics-Apps auf Geräten und dem Netzwerk Ihres Unternehmens herstellen.
- Wenn Sie BlackBerry Connectivity Node installieren, kann BlackBerry Secure Gateway eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum Mailserver Ihres Unternehmens für iOS-Geräte bereitstellen.

Dieses Diagramm zeigt die möglichen Datenpfade.

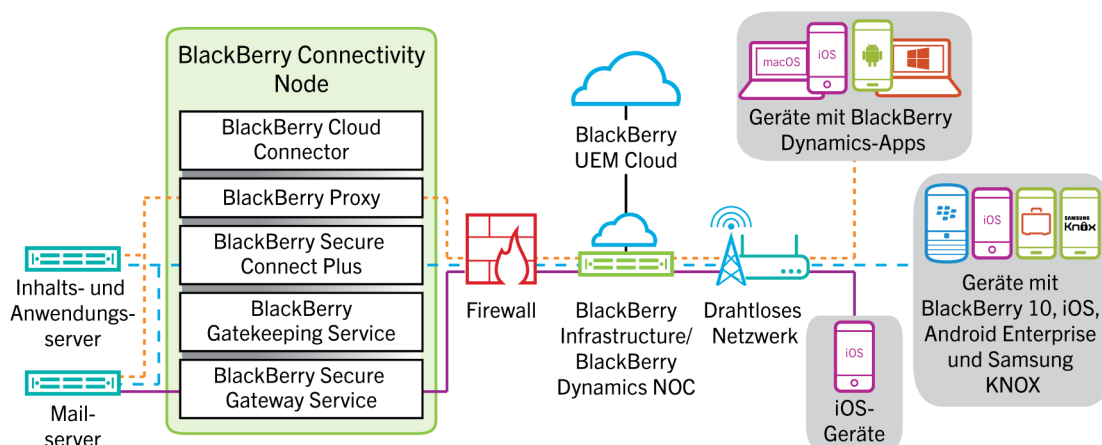


Senden und Empfangen von geschäftlichen Daten über BlackBerry UEM Cloud und die BlackBerry Infrastructure

Wenn Sie BlackBerry Connectivity Node installieren, können Geräte über BlackBerry UEM Cloud und die BlackBerry Infrastructure oder die BlackBerry Dynamics NOC mithilfe der folgenden Dienste eine Verbindung zu den Ressourcen Ihres Unternehmens herstellen:

| Dienst | Beschreibung |
|--------------------------------|--|
| BlackBerry Secure Connect Plus | <p>BlackBerry Secure Connect Plus stellt über die BlackBerry Infrastructure einen sicheren IP-Tunnel zwischen Apps und dem Netzwerk des Unternehmens bereit, um Daten zu übertragen.</p> <p>Für Android Enterprise-Geräte bietet BlackBerry Secure Connect Plus einen sicheren Tunnel zwischen Apps für den geschäftlichen Bereich und dem Netzwerk Ihres Unternehmens.</p> <p>Für Samsung Knox Workspace-Geräte kann BlackBerry Secure Connect Plus einen sicheren Tunnel zwischen Ihrem Unternehmensnetzwerk und allen geschäftlichen Apps oder nur den angegebenen geschäftlichen Apps bereitstellen.</p> <p>Für iOS-Geräte kann BlackBerry Secure Connect Plus einen sicheren Tunnel zwischen Ihrem Unternehmensnetzwerk und allen Apps oder nur den angegebenen Apps bereitstellen.</p> |
| BlackBerry Proxy | <p>BlackBerry Proxy bietet eine sichere Verbindung zwischen BlackBerry Dynamics Apps auf Geräten und Ressourcen Ihres Unternehmens hinter der Firewall. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen von BlackBerry Dynamics NOC ermöglicht.</p> |
| BlackBerry Secure Gateway | <p>Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum E-Mail-Server Ihres Unternehmens für iOS-Geräte.</p> |

Das folgende Diagramm zeigt, wie Geräte über die BlackBerry Infrastructure und BlackBerry UEM Cloud eine Verbindung zu den Ressourcen Ihres Unternehmens herstellen können.

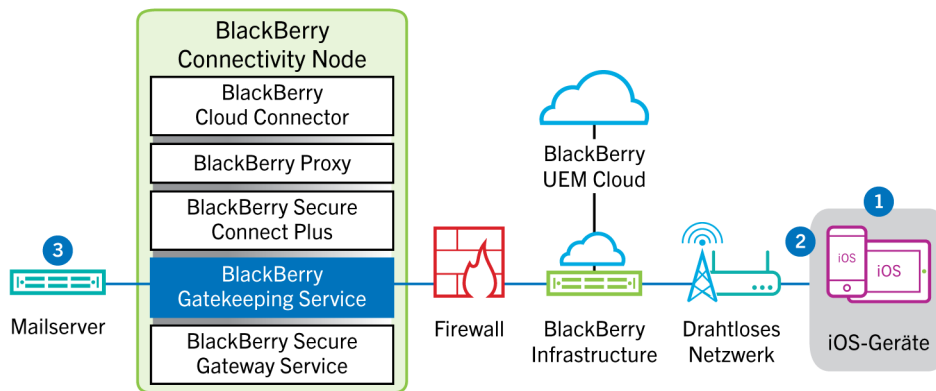


Weitere Informationen zum Aktivieren von BlackBerry Secure Connect Plus finden Sie unter „Aktivieren und Konfigurieren von BlackBerry Secure Connect Plus“ in der Dokumentation für Administratoren.

Weitere Informationen zum Aktivieren des BlackBerry Secure Gateway finden Sie unter „Schützen von E-Mail-Daten mithilfe von BlackBerry Secure Gateway“ in der Dokumentation für Administratoren.

Datenfluss: Senden einer E-Mail von einem iOS-Gerät mithilfe des BlackBerry Secure Gateway

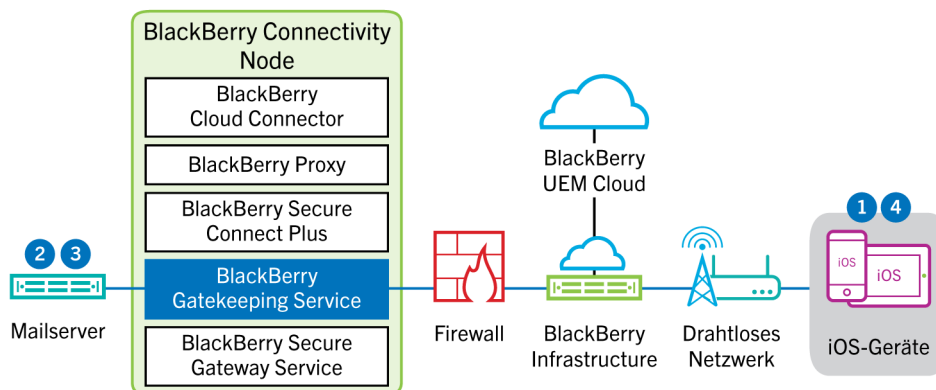
Dieser Datenfluss beschreibt, wie geschäftliche E-Mail- und Kalenderdaten von iOS-Geräten mithilfe des BlackBerry Secure Gateway zum Exchange ActiveSync-Server übertragen werden.



1. Ein Benutzer erstellt eine E-Mail oder aktualisiert ein Terminplanelement im geschäftlichen Bereich.
2. Das neue oder geänderte Element wird vom Gerät über die BlackBerry Infrastructure und den BlackBerry Secure Gateway an den E-Mail-Server gesendet.
3. Der E-Mail-Server aktualisiert die Terminplannerdaten im Postfach des Benutzers oder sendet das E-Mail-Element an den Empfänger und eine Bestätigung an das Gerät.

Datenfluss: Empfangen einer E-Mail auf einem iOS-Gerät mithilfe von BlackBerry Secure Gateway

Dieser Datenfluss beschreibt, wie geschäftliche E-Mail- und Kalenderdaten zwischen iOS-Geräten und dem Exchange ActiveSync-Server mithilfe des BlackBerry Secure Gateway übertragen werden.

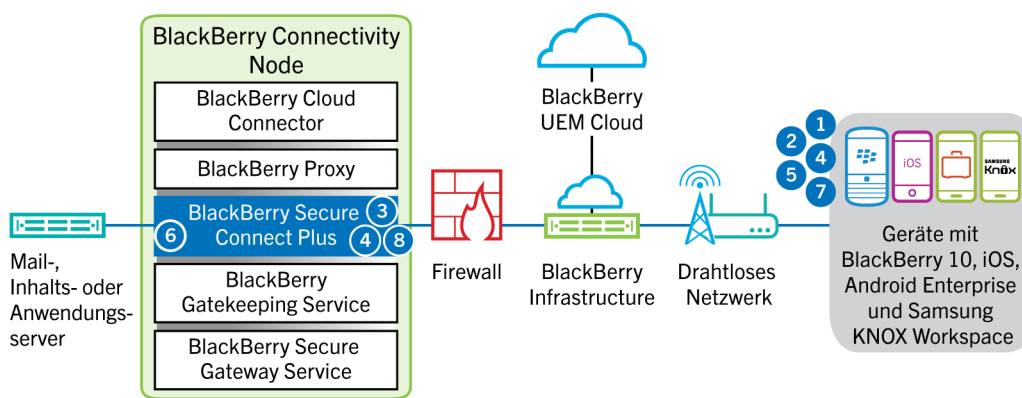


1. Das Gerät sendet eine HTTPS-Anforderung an den E-Mail-Server und fordert diesen auf, das Gerät zu benachrichtigen, wenn sich Elemente in den Ordnern ändern, die für die Synchronisierung konfiguriert sind. Die Anforderung wird über den verschlüsselten und authentifizierten Kanal zwischen der BlackBerry Infrastructure und dem BlackBerry Secure Gateway zum E-Mail-Server geleitet.

2. Werden in diesem Intervall keine neuen oder geänderten Elemente gefunden, sendet der E-Mail-Server die Meldung „HTTP 200 OK“ an das Gerät. Das Gerät gibt eine neue Anforderung aus, und der Vorgang beginnt von vorne.
3. Sind für das Gerät neue oder geänderte Elemente vorhanden, wie eine neue E-Mail oder ein aktualisierter Kalendereintrag, sendet der E-Mail-Server die Updates über den sicheren Kanal zwischen dem BlackBerry Secure Gateway und der BlackBerry Infrastructure an die E-Mail- oder Terminplaner-App auf dem Gerät.
4. Nach Abschluss der Synchronisierung sendet das Gerät eine weitere Anforderung, um den Prozess neu zu starten.

Datenfluss: Senden und Empfangen von geschäftlichen Daten mit BlackBerry Secure Connect Plus

Dieser Datenfluss beschreibt, wie Daten übertragen werden, wenn eine App auf einem Gerät, das für die Verwendung von BlackBerry Secure Connect Plus konfiguriert ist, auf einen Anwendungs- oder Inhaltsserver Ihres Unternehmens zugreift.



1. Der Benutzer öffnet eine App zum Zugriff auf geschäftliche Daten auf einem Inhalts- oder Anwendungsserver, der sich hinter der Firewall Ihres Unternehmens befindet.
 - Auf Android Enterprise- und Samsung Knox Workspace-Geräten können alle geschäftlichen Apps BlackBerry Secure Connect Plus verwenden.
 - Auf iOS-Geräten legen Sie fest, ob alle Anwendungen oder nur bestimmte Apps BlackBerry Secure Connect Plus verwenden können.
2. Das Gerät erkennt, dass ein sicherer IP-Tunnel die direkteste und kostengünstigste Methode ist, um eine Verbindung zum Anwendungs- oder Inhaltsserver zum Abrufen der Daten herzustellen, und sendet eine Anforderung über Port 443 durch einen TLS-Tunnel an die BlackBerry Infrastructure, um einen sicheren Tunnel für das geschäftliche Netzwerk aufzubauen. Das Signal wird standardmäßig mit FIPS-140-zertifizierten Certicom-Bibliotheken verschlüsselt. Der Tunnel für das Signal ist komplett verschlüsselt.
3. BlackBerry Secure Connect Plus empfängt die Anforderung von der BlackBerry Infrastructure über Port 3101.
4. Das Gerät und BlackBerry Secure Connect Plus handeln die Tunnelparameter aus und erstellen einen sicheren Tunnel für das Gerät durch die BlackBerry Infrastructure. Der Tunnel ist authentifiziert und durchgehend mit DTLS verschlüsselt.
5. Die App verwendet den Tunnel für die Verbindung mit dem Anwendungs- oder Inhaltsserver unter Verwendung standardmäßiger IPv4-Protokolle (TCP und UDP).
6. BlackBerry Secure Connect Plus überträgt die IP-Daten zu und vom Netzwerk des Unternehmens. BlackBerry Secure Connect Plus verschlüsselt und entschlüsselt den Datenverkehr mit FIPS-140-zertifizierten Certicom-Bibliotheken.
7. Die App empfängt die Daten und zeigt sie auf dem Gerät an.
8. Solange der Tunnel geöffnet ist, wird er von unterstützten Apps für den Zugriff auf Netzwerkressourcen verwendet. Wenn der Tunnel nicht mehr die beste verfügbare Methode ist, um eine Verbindung mit dem Unternehmensnetzwerk herzustellen, wird er von BlackBerry Secure Connect Plus beendet.

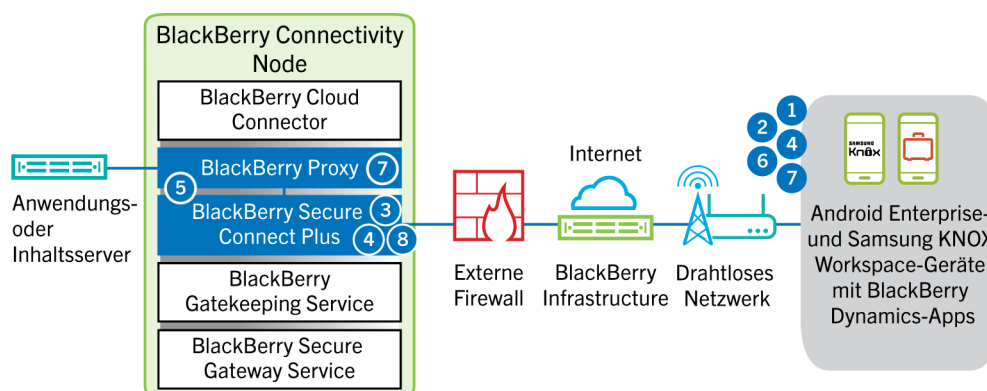
Wenn Sie für iOS-Geräte Per App VPN für BlackBerry Secure Connect Plus konfigurieren und keine der konfigurierten Apps verwendet werden, wird der Tunnel schließlich geschlossen.

Datenfluss: Senden und Empfangen von geschäftlichen Daten von einer BlackBerry Dynamics-App auf einem Android-Gerät unter Verwendung von BlackBerry Secure Connect Plus

Dieser Datenfluss beschreibt, wie die Daten übertragen werden, wenn eine BlackBerry Dynamics-App auf einem Android Enterprise- oder Samsung Knox Workspace-Gerät BlackBerry Secure Connect Plus verwendet.

Wenn Sie BlackBerry Secure Connect Plus mit BlackBerry Dynamics-Apps auf einem Android Enterprise-Gerät verwenden, wird empfohlen, dass Sie BlackBerry Dynamics-Apps an der Verwendung von BlackBerry Secure Connect Plus hindern, um Netzwerklatenz zu vermeiden. Sie können keine spezifischen Apps auf Samsung Knox Workspace-Geräten sperren.

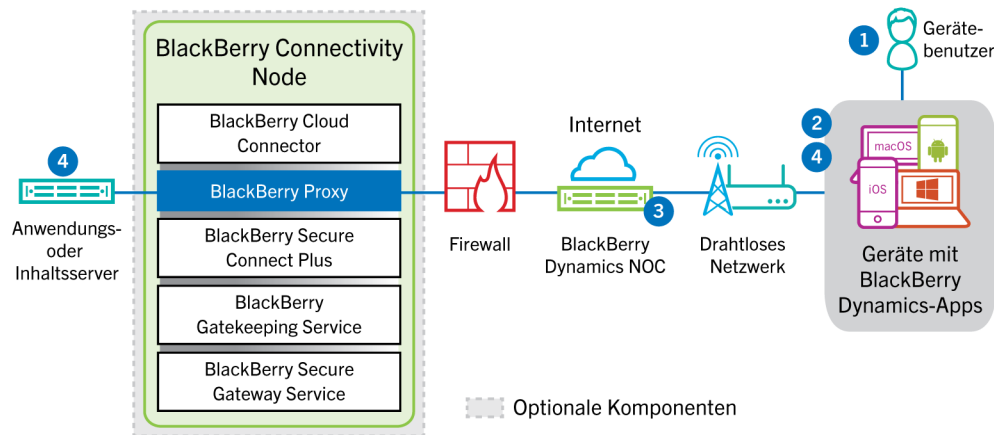
Wenn Sie BlackBerry Secure Connect Plus mit BlackBerry Dynamics-Apps auf einem Android Enterprise-Gerät oder ein Samsung Knox Workspace-Gerät verwenden, wird empfohlen, dass Sie BlackBerry UEM konfigurieren, damit sie keine BlackBerry Dynamics-App-Daten über BlackBerry Dynamics NOC sendet, um Netzwerklatenz zu vermeiden.



1. Der Benutzer öffnet eine BlackBerry Dynamics-App, um auf geschäftliche Daten zuzugreifen.
2. Das Gerät sendet eine Anfrage über einen TLS-Tunnel und Port 443 an die BlackBerry Infrastruktur, um einen sicheren Tunnel zum Netzwerk des Unternehmens anzufordern. Das Signal wird standardmäßig mit FIPS-140-zertifizierten Certicom-Bibliotheken verschlüsselt. Der Tunnel für das Signal ist komplett verschlüsselt.
3. BlackBerry Secure Connect Plus empfängt die Anforderung von der BlackBerry Infrastruktur über Port 3101.
4. Das Gerät und BlackBerry Secure Connect Plus handeln die Tunnelparameter aus und erstellen einen sicheren Tunnel für das Gerät durch die BlackBerry Infrastruktur. Der Tunnel ist authentifiziert und durchgehend mit DTLS verschlüsselt.
5. BlackBerry Secure Connect Plus stellt eine Verbindung mit BlackBerry Proxy her.
6. Die BlackBerry Dynamics-App baut eine Verbindung mit BlackBerry Proxy über den BlackBerry Secure Connect Plus-Tunnel auf.
7. BlackBerry Proxy authentifiziert sich mit seinem Serverzertifikat bei der BlackBerry Dynamics-App. BlackBerry Proxy überprüft die App anhand eines MAC, der mit einem Sitzungsschlüssel verschlüsselt und nur BlackBerry Proxy und der App bekannt ist.
8. Wenn die sichere Verbindung zwischen BlackBerry Proxy und der App hergestellt wurde, können die geschäftlichen Daten zwischen dem Gerät und den Anwendungs- und Inhaltsservern hinter der Firewall über den BlackBerry Secure Connect Plus-Tunnel oder BlackBerry Proxy übertragen werden. BlackBerry Secure Connect Plus verschlüsselt und entschlüsselt den Datenverkehr mit FIPS-140-zertifizierten Certicom-Bibliotheken.

Datenfluss: Senden und Empfangen von geschäftlichen Daten von einer BlackBerry Dynamics-App

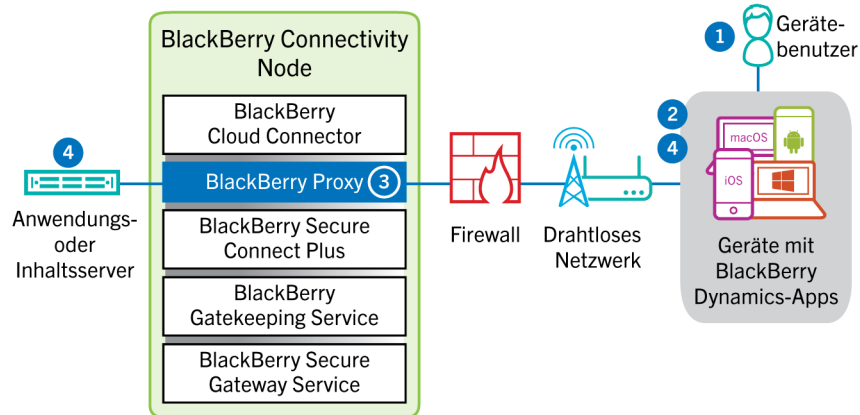
Dieser Datenfluss beschreibt, wie Daten übertragen werden, wenn eine BlackBerry Dynamics-App auf einen Anwendungs- oder Inhaltsserver in Ihrem Unternehmen zugreift.



1. Der Benutzer öffnet eine BlackBerry Dynamics-App, um auf geschäftliche Daten zuzugreifen.
2. Die BlackBerry Dynamics-App baut eine Verbindung mit dem BlackBerry Dynamics NOC auf. Die Verbindung wird mit dem Master-Verbindungsschlüssel authentifiziert, der während der Aktivierung der App erzeugt wurde.
3. Das BlackBerry Dynamics NOC führt eine der folgenden Aktionen aus:
 - a. Kommuniziert mit BlackBerry Proxy über eine zuvor erstellte sichere Verbindung, die den Aufbau einer durchgehenden Verbindung über Port 443 für geschäftliche Daten zwischen der BlackBerry Dynamics-App und BlackBerry Proxy ermöglicht. Die geschäftlichen Daten werden mit einem Sitzungsschlüssel verschlüsselt, der dem BlackBerry Dynamics NOC nicht bekannt ist.
 - b. Wenn der BlackBerry Connectivity Node nicht konfiguriert ist, kommuniziert er direkt mit Ihrem Anwendungs- oder Inhaltsserver über einen Port, den Sie in der Firewall Ihres Unternehmens geöffnet haben.
4. Wenn der BlackBerry Connectivity Node konfiguriert ist, sobald eine sichere durchgehende Verbindung zwischen dem BlackBerry Dynamics NOC und BlackBerry Proxy besteht, können die geschäftlichen Daten zwischen dem Gerät und den Anwendungs- und Inhaltsservern hinter der Firewall über BlackBerry Proxy übertragen werden.

Datenfluss: Senden und Empfangen von geschäftlichen Daten von einer BlackBerry Dynamics-App unter Verwendung von BlackBerry Dynamics Direct Connect

Dieser Datenfluss beschreibt, wie Daten übertragen werden, wenn eine BlackBerry Dynamics-App auf einen Anwendungs- oder einen Inhaltsserver in Ihrem Unternehmen über BlackBerry Dynamics Direct Connect und BlackBerry Proxy zugreift.

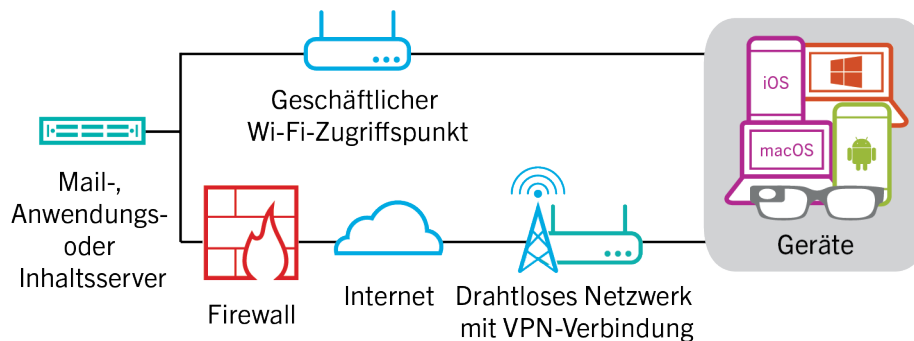


1. Der Benutzer öffnet eine BlackBerry Dynamics-App, um auf geschäftliche Daten zuzugreifen.
2. Die BlackBerry Dynamics-App stellt eine TLS-Verbindung zu BlackBerry Proxy über Port 17533 her.
3. BlackBerry Proxy authentifiziert sich bei der BlackBerry Dynamics-App. BlackBerry Proxy authentifiziert sich mit seinem Serverzertifikat bei der App. BlackBerry Proxy überprüft die App anhand eines MAC, der mit einem Sitzungsschlüssel verschlüsselt und nur BlackBerry Proxy und der App bekannt ist.
4. Wenn eine sichere durchgehende Verbindung besteht, können die geschäftlichen Daten zwischen dem Gerät und den Anwendungs- und Inhaltsservern hinter der Firewall über den BlackBerry Proxy übertragen werden.

Senden und Empfangen von geschäftlichen Daten über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk

Geräte, bei denen entweder Sie oder andere Benutzer VPN- oder Wi-Fi-Profile konfiguriert haben, können ggf. nicht mithilfe des VPNs Ihres Unternehmens oder Ihres Wi-Fi-Geschäftsnetzwerks auf die Ressourcen Ihres Netzwerks zugreifen. Zur Verwendung des Unternehmens-VPNs müssen Benutzer mit einem Android-Gerät mit der Aktivierungsart „MDM-Steuerelemente“ oder Samsung Knox Workspace das VPN-Profil auf ihren Geräten manuell konfigurieren.

Dieses Diagramm stellt dar, wie Daten übertragen werden können, wenn ein Gerät sich mit den Ressourcen Ihres Unternehmens mithilfe des VPNs Ihres Unternehmens oder des Wi-Fi-Geschäftsnetzwerks verbindet.

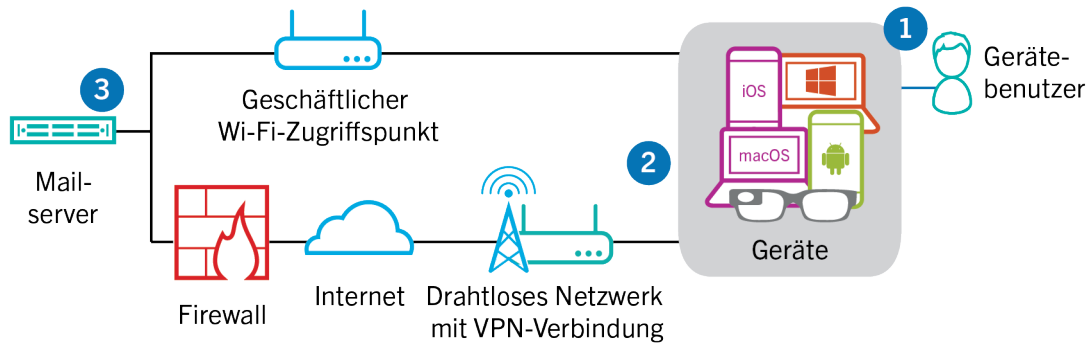


In der folgenden Tabelle wird beschrieben, wann Geräte über das VPN oder das geschäftliche Wi-Fi-Netzwerk Ihres Unternehmens eine Verbindung mit dem Unternehmensnetzwerk herstellen.

| Gerätetyp | Beschreibung |
|---|--|
| Android Enterprise-Geräte und Knox Workspace-Geräte | Standardmäßig nutzen Android Enterprise- und Knox Workspace-Geräte Ihr Unternehmens-VPN oder geschäftliches Wi-Fi-Netzwerk nur dann zum Senden und Empfangen von geschäftlichen Daten, wenn BlackBerry Secure Connect Plus nicht aktiviert ist. |
| Windows- und macOS-Geräte sowie Android-Geräte mit der Aktivierungsart MDM-Steuerelemente | Windows- und macOS-Geräte sowie Android-Geräte mit der Aktivierungsart MDM-Steuerelemente, die das VPN oder das geschäftliche Wi-Fi-Netzwerk Ihres Unternehmens zum Senden und Empfangen von Geschäftsdaten verwenden. Um das VPN Ihres Unternehmens zu verwenden, müssen die Android-Benutzer manuell ein VPN-Profil auf ihren Geräten konfigurieren. |
| iOS | iOS-Geräte nutzen das VPN Ihres Unternehmens oder das geschäftliche Wi-Fi-Netzwerk zum Senden und Empfangen von Exchange ActiveSync-Daten, wenn der BlackBerry Secure Gateway nicht aktiviert ist. Für alle anderen geschäftlichen Daten wird das VPN Ihres Unternehmens oder das geschäftliche Wi-Fi-Netzwerk verwendet. |

Datenfluss: Senden einer E-Mail von einem Gerät über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk

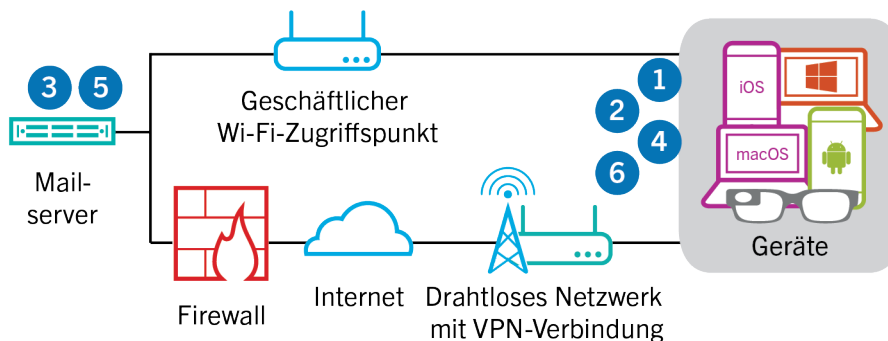
Dieser Datenfluss beschreibt, wie E-Mail- und Kalenderdaten von dem Gerät zum E-Mail-Server über das VPN Ihres Unternehmens oder das geschäftliche Wi-Fi-Netzwerk mithilfe von Exchange ActiveSync übertragen werden.



1. Ein Benutzer erstellt eine E-Mail oder aktualisiert ein Terminplanerelement im geschäftlichen Bereich.
2. Das Gerät sendet das neue oder geänderte Element an den E-Mail-Server über das VPN Ihres Unternehmens oder das Wi-Fi-Geschäftsnetzwerk.
3. Der E-Mail-Server aktualisiert die Terminplanerdaten im Postfach des Benutzers oder sendet das E-Mail-Element an den Empfänger und eine Bestätigung an das Gerät.

Datenfluss: Empfangen einer E-Mail auf einem Gerät über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk

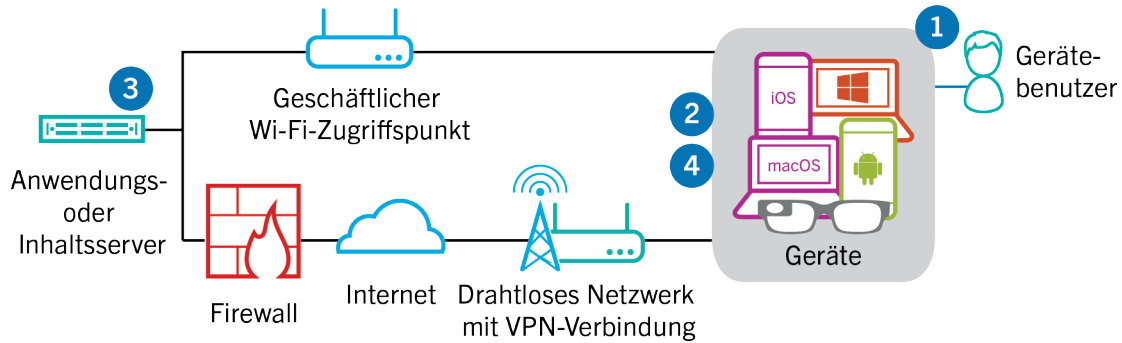
Dieser Datenfluss beschreibt, wie E-Mail- und Kalenderdaten von dem Gerät zum E-Mail-Server über das VPN Ihres Unternehmens oder das geschäftliche Wi-Fi-Netzwerk mithilfe von Exchange ActiveSync übertragen werden.



1. Das Gerät sendet eine HTTPS-Anforderung an den E-Mail-Server und fordert diesen auf, das Gerät zu benachrichtigen, wenn sich Elemente in den Ordnern ändern, die für die Synchronisierung konfiguriert sind. Die Anforderung wird über das VPN Ihres Unternehmens oder das Wi-Fi-Geschäftsnetzwerk an den E-Mail-Server geleitet.
2. Das Gerät befindet sich im Standbymodus.
3. Sind für das Gerät neue oder geänderte Elemente vorhanden, wie eine neue E-Mail oder ein aktualisierter Kalendereintrag, sendet der E-Mail-Server die Updates an das Gerät. Die neuen oder geänderten Elemente werden über das VPN- oder geschäftliche Wi-Fi-Netzwerk Ihrer Organisation an die E-Mail- bzw. Terminplanerdaten-App auf dem Gerät übertragen.
4. Nach Abschluss der Synchronisierung sendet das Gerät eine weitere Anforderung, um den Prozess neu zu starten.
5. Werden in diesem Intervall keine neuen oder geänderten Elemente gefunden, sendet der Mail- oder Anwendungsserver über das Exchange ActiveSync-Protokoll eine Meldung an das Gerät.
6. Das Gerät gibt eine neue Anforderung aus, und der Vorgang beginnt von vorne.

Datenfluss: Zugreifen auf einen Anwendungs- oder Inhaltsserver über ein VPN oder ein geschäftliches Wi-Fi-Netzwerk

Dieser Datenfluss beschreibt, wie Daten zwischen einem Anwendungs- oder einem Inhaltsserver in Ihrem Unternehmen und einer App auf einem Gerät mithilfe einer VPN-Verbindung oder eines Wi-Fi-Geschäftsnetzwerks übertragen werden.



1. Der Benutzer öffnet eine geschäftliche App, um geschäftliche Daten anzuzeigen. Der Benutzer öffnet beispielsweise den Work Browser, um im Intranet zu surfen, oder verwendet eine intern entwickelte App, um auf die Kundendaten Ihres Unternehmens zuzugreifen.
2. Die App stellt eine Verbindung mit dem Anwendungs- oder Inhaltsserver her, um die Daten abzurufen. Die Anforderung wird über das VPN Ihres Unternehmens oder das Wi-Fi-Geschäftsnetzwerk an den Anwendungs- oder Inhaltsserver geleitet.
3. Der Anwendungs- oder Inhaltsserver antwortet mit den geschäftlichen Daten. Die geschäftlichen Daten werden über Ihr VPN oder Ihr geschäftliches Wi-Fi-Netzwerk an die App im geschäftlichen Bereich auf dem Gerät geleitet:
4. Die App empfängt die Daten und zeigt sie auf dem Gerät an.

Rechtliche Hinweise

©2022 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE 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.

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, GARANTIEEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIEEN, 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 DRITTPRODUKTEN UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE, VERSCHÄRFTEN SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE,

STRAFE EINSCHLIESSENDE SCHÄDEN, FOLGESCHÄDEN ODER SCHÄDEN, FÜR DIE ANSPRUCH AUF KOMPENSATORISCHEN SCHADENERSATZ BESTEHT, SCHÄDEN WEGEN ENTGANGENEN GEWINNEN ODER EINKOMMEN, NICHTREALISIERUNG ERWARTETER EINSPARUNGEN, BETRIEBSUNTERBRECHUNGEN, VERLUST GESCHÄFTLICHER DATEN, ENTGANGENE GESCHÄFTSCHANCEN ODER BESCHÄDIGUNG BZW. VERLUST VON DATEN, DAS UNVERMÖGEN, DATEN ZU ÜBERTRAGEN ODER ZU EMPFANGEN, PROBLEME IM ZUSAMMENHANG MIT ANWENDUNGEN, DIE IN VERBINDUNG MIT BLACKBERRY-PRODUKTEN UND -DIENSTEN VERWENDET WERDEN, KOSTEN VON AUSFALLZEITEN, NICHTVERWENDBARKEIT VON BLACKBERRY-PRODUKTEN UND -DIENSTEN ODER TEILEN DAVON BZW. VON MOBILFUNKDIENSTEN, KOSTEN VON ERSATZGÜTERN, DECKUNG, EINRICHTUNGEN ODER DIENSTEN, KAPITAL- ODER ANDERE VERMÖGENSSCHÄDEN, UNABHÄNGIG DAVON, OB SCHÄDEN DIESER ART ABZUSEHEN ODER NICHT ABZUSEHEN WAREN, UND AUCH DANN, WENN BLACKBERRY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

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

DIE IN DIESEM DOKUMENT GENANNTE EINSCHRÄNKUNGEN, AUSSCHLÜSSE UND HAFTUNGSAUSSCHLÜSSE GELTEN (A) UNGEACHTET DER VON IHNEN ANGEFÜHRTE 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 GRUNDLEGENDE ZWECK DIESER VEREINBARUNG ODER EINES DARIN ENTHALTENEN RECHTSBEHELFS WIRKSAM; UND GELTEN (B) FÜR BLACKBERRY UND DIE ZUGEHÖRIGEN UNTERNEHMEN, RECHTSNACHFOLGER, BEVOLLMÄCHTIGTE, VERTRETER, LIEFERANTE (EINSCHLIESSLICH MOBILFUNKANBIETERN), AUTORISIERTE BLACKBERRY-DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH MOBILFUNKANBIETERN) UND DIE JEWEILIGEN FÜHRUNGSKRÄFTE, ANGESTELLTE UND UNABHÄNGIGE AUFTRAGNEHMER.

ZUSÄTZLICH ZU DEN OBEN GENANNTE EINSCHRÄNKUNGEN UND AUSSCHLÜSSEN HAFTEN DIE FÜHRUNGSKRÄFTE, ANGESTELLTE, VERTRETER, DISTRIBUTOREN, LIEFERANTE, UNABHÄNGIGE 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 GARANTIE, DIE VON BLACKBERRY FÜR TEILE VON BELIEBIGEN BLACKBERRY-PRODUKTEN ODER -DIENSTLEISTUNGEN AN ANDERER STELLE ALS IN DIESER DOKUMENTATION ANGEGEBEN WURDEN, ZU ERSETZEN.

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

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

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

Veröffentlicht in Kanada