BlackBerry UEM

Architektur und Datenflüsse

12.12

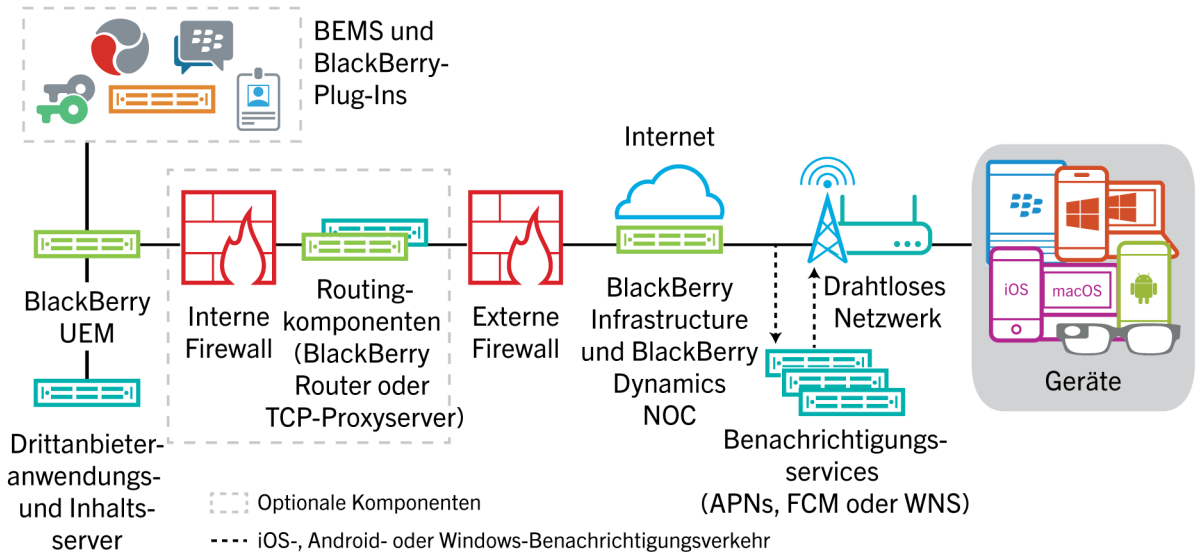
Inhalt

BlackBerry UEM-Architektur und -Datenflüsse

BlackBerry UEM ist eine plattformübergreifende EMM-Lösung von BlackBerry, die umfassende Funktionen für die Verwaltung von Geräten und Anwendungen sowie für das Content Management mit integrierter Sicherheit und Konnektivität bietet und Sie bei der Verwaltung von iOS-, macOS-, Android-, Windows 10- und BlackBerry 10-Geräten in Ihrem Unternehmen unterstützt.

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

Architektur: BlackBerry UEM-Lösung



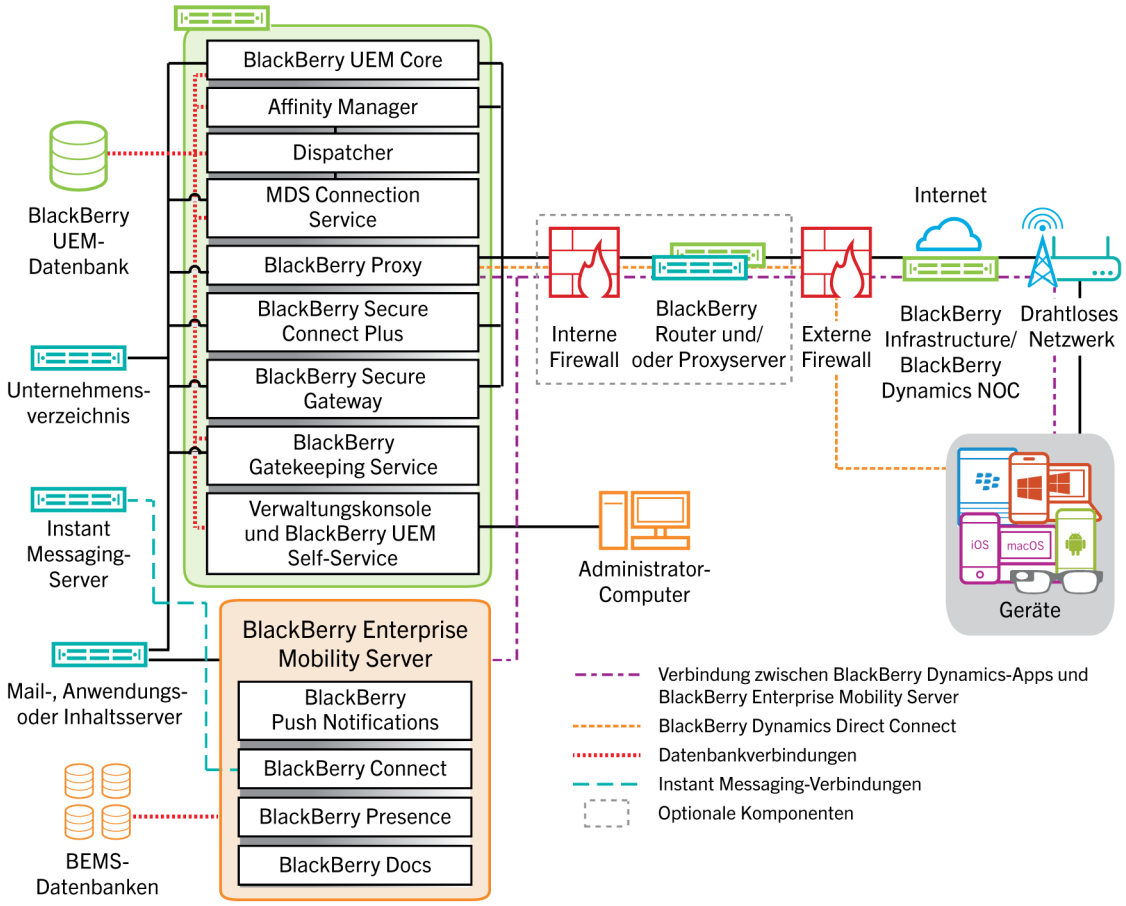
Komponente	Beschreibung
BlackBerry UEM	BlackBerry UEM ist eine einheitliche Endpunktverwaltungslösung, die umfassende Funktionen für die plattformübergreifende Verwaltung von Geräten und Anwendungen sowie für das Content Management mit integrierter Sicherheit und Konnektivität bietet.

Komponente	Beschreibung
BlackBerry Infrastructure	Die BlackBerry Infrastructure ist ein globales privates Datennetzwerk, das über zahlreiche Regionen verteilt wird und Daten während der Übertragung zwischen Tausenden von Unternehmen und Millionen von Benutzern weltweit sichert. Sie ist darauf ausgelegt, den Transport von Daten zwischen BlackBerry-Diensten und Endbenutzergeräten effizient zu verwalten. Für Unternehmen mit BlackBerry UEM registriert die BlackBerry Infrastructure Benutzerinformationen für die Geräteaktivierung, überprüft Lizenzinformationen für BlackBerry UEM und stellt einen vertrauenswürdigen Pfad, der auf einer starken, kryptografischen gegenseitigen Authentifizierung basiert, zwischen dem Unternehmen und jedem Benutzer bereit. Aufgrund der durchgehenden Verschlüsselung, die Daten schützt, die zwischen dem Gerät und BlackBerry UEM übertragen werden, ermöglicht BlackBerry UEM eine konstante Verbindung zur BlackBerry Infrastructure. Dies gewährleistet, dass Unternehmen nur eine einzelne ausgehende Verbindung zu einer vertrauenswürdigen IP-Adresse benötigen, um Daten an Benutzer zu senden. Alle Daten zwischen der BlackBerry Infrastructure und BlackBerry UEM werden authentifiziert und verschlüsselt, um für Geräte außerhalb der Firewall einen sicheren Kommunikationskanal in Ihr Unternehmen bereitzustellen.
BlackBerry Dynamics NOC	Das BlackBerry Dynamics NOC ist ein Netzwerkbetriebszentrum, das eine sichere Kommunikation zwischen den BlackBerry Dynamics-Apps auf Geräten und BlackBerry UEM, sowie dem BlackBerry Enterprise Mobility Server ermöglicht.
Geräte	BlackBerry UEM unterstützt Geräte mit iOS, macOS, Android, Windows 10 und BlackBerry 10.
Benachrichtigungsdienste	BlackBerry UEM 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. • 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. • Windows-Pushbenachrichtungsdienst (WNS) ist ein Microsoft-Dienst zum Senden von Benachrichtigungen an Windows-Geräte.

Komponente	Beschreibung
Routingkomponenten	Standardmäßig stellt BlackBerry UEM über die Ports 3101 und 443 eine direkte Verbindung mit der BlackBerry Infrastructure her, sodass Sie keine weiteren Routingkomponenten installieren müssen. Wenn die Sicherheitsrichtlinie Ihres Unternehmens jedoch vorschreibt, dass interne Systeme keine direkten Verbindungen mit dem Internet herstellen dürfen, können Sie den BlackBerry Router oder einen Proxyserver verwenden. Der BlackBerry Router agiert als Proxy-Server für Verbindungen über die BlackBerry Infrastructure zwischen BlackBerry UEM und allen Geräten. Der BlackBerry Router kann SOCKs v5 ohne Authentifizierung unterstützen. Wenn Ihr Unternehmen schon einen TCP-Proxy-Server installiert hat oder einen benötigt, um die Netzwerkanforderungen zu erfüllen, können Sie einen TCP-Proxy-Server anstelle des BlackBerry Router verwenden. Der TCP-Proxy-Server kann SOCKs v5 ohne Authentifizierung unterstützen. Der BlackBerry UEM Core und BlackBerry Proxy unterstützen das Herstellen von Verbindungen mit dem BlackBerry Dynamics NOC über einen HTTP-Proxyserver.
Drittanbieteranwendungs- und Inhaltsserver	Zusätzliche Inhaltsserver und Anwendungsserver in der Unternehmensumgebung, einschließlich Unternehmensverzeichnis, Mailserver, Zertifizierungsstellen usw.
BlackBerry-Plug-ins und BEMS	BlackBerry UEM arbeitet mit zusätzlichen BlackBerry Unternehmensprodukten zusammen, z. B. BlackBerry 2FA und BlackBerry Enterprise Identity, um Ihnen die Erweiterung der UEM-Funktionen in Ihrem Unternehmen zu ermöglichen. Der BlackBerry Enterprise Mobility Server stellt verschiedene Dienste bereit, die zum Übertragen von geschäftlichen Daten zwischen BlackBerry Dynamics-Apps verwendet werden.

BlackBerry UEM-Komponenten

Dieses Diagramm zeigt, wie die BlackBerry UEM-Komponenten miteinander verbunden sind, wenn alle Komponenten in der einfachsten Konfiguration des Produkts gemeinsam installiert werden.



Weitere Informationen zu den für Verbindungen zwischen den Komponenten verwendeten Ports finden Sie in der Dokumentation zur Planung unter „Konfigurieren von Ports“.

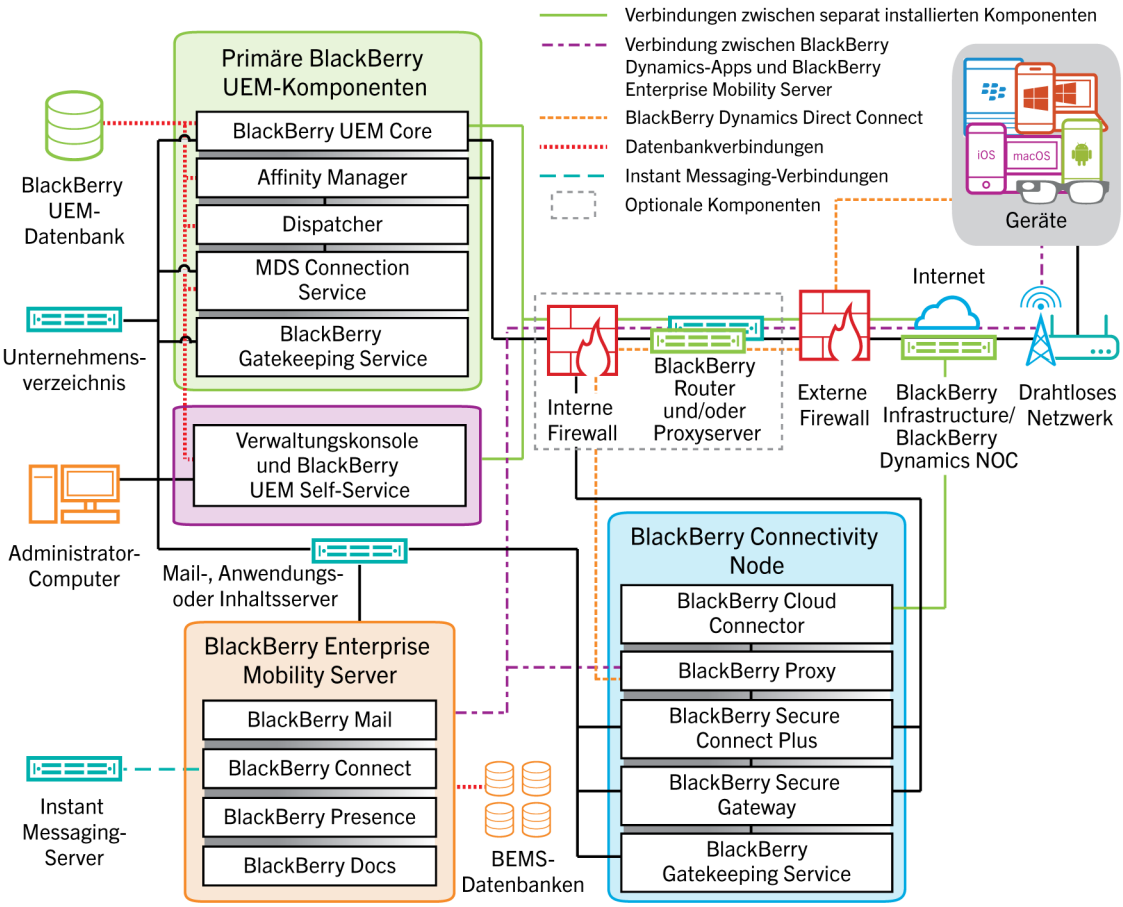
Komponentenname	Beschreibung
BlackBerry UEM Core	BlackBerry UEM Core ist die zentrale Komponente der BlackBerry UEM-Architektur. Er weist mehrere Unterkomponenten auf, die verantwortlich sind für: • Protokollierung, Überwachung, Reporting und Verwaltungsfunktionen • Authentifizierungs- und Autorisierungsdienste • Planen und Senden von Befehlen, IT-Richtlinien und Profilen an Geräte • Sendet Benutzer-, Richtlinien- und andere Konfigurationsdaten an die auf Geräten installierten BlackBerry Dynamics-Apps.
BlackBerry UEM-Datenbank	Die BlackBerry UEM-Datenbank ist eine relationale Datenbank, die Informationen zum Benutzerkonto und der Konfiguration enthält, die von BlackBerry UEM für die Verwaltung von Geräten und BlackBerry Dynamics-Apps verwendet werden.

Komponentenname	Beschreibung
BlackBerry MDS Connection Service	Der BlackBerry MDS Connection Service stellt eine sichere Verbindung zwischen BlackBerry 10-Geräten und dem Netzwerk Ihres Unternehmens bereit, wenn das Gerät nicht mit Ihrem Wi-Fi-Geschäftsnetzwerk verbunden ist oder eine VPN-Verbindung verwendet.
BlackBerry Dispatcher	Der BlackBerry Dispatcher stellt sichere Konnektivität unter Verwendung von IPPP für BlackBerry 10-Geräte bereit.
BlackBerry Affinity Manager	Der BlackBerry Affinity Manager ist für die Aufrechterhaltung einer aktiven SRP-Verbindung zwischen BlackBerry 10-Geräten und der BlackBerry Infrastructure verantwortlich, wenn diese Geräte BlackBerry Secure Connect Plus nicht verwenden.
BlackBerry Proxy	Der BlackBerry Proxy sorgt für eine sichere Verbindung zwischen Ihrem Unternehmen und dem BlackBerry Dynamics NOC. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen des BlackBerry Dynamics NOC ermöglicht.
BlackBerry Secure Connect Plus	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.
BlackBerry Secure Gateway	Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum E-Mail-Server Ihres Unternehmens für iOS-Geräte.
BlackBerry Gatekeeping Service	Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf BlackBerry UEM 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.
Verwaltungskonsole und BlackBerry UEM Self-Service	Die Verwaltungskonsole und der BlackBerry UEM Self-Service bilden eine webbasierte Konsole, die Administrator- und Benutzerzugriff auf BlackBerry UEM ermöglicht. Sie können Systemeinstellungen, Benutzer, Geräte und Apps über die Verwaltungskonsole verwalten. Benutzer können den BlackBerry UEM Self-Service verwenden, um ein Aktivierungskennwort einzurichten und Befehle, z. B. zum Einrichten des Kennworts, Sperren des Geräts und Löschen von Gerätedaten, an Geräte zu senden.
BlackBerry Enterprise Mobility Server	BEMS führt verschiedene Dienste zusammen, die zum Senden und Empfangen von Daten von BlackBerry Dynamics-Apps verwendet werden, z. B. BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence und BlackBerry Docs.

Komponentenname	Beschreibung
BlackBerry Enterprise Mobility Server-Datenbanken	In den BEMS-Datenbanken werden Benutzer-, App-, Richtlinien- und Konfigurationsinformationen gespeichert.
BlackBerry Push Notifications	BlackBerry Push Notifications 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.
BlackBerry Connect	BlackBerry Connect ermöglicht sicheres Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen auf iOS- und Android-Geräten.
BlackBerry Presence	BlackBerry Presence stellt Informationen zum Anwesenheitsstatus für BlackBerry Dynamics-Apps in Echtzeit bereit.
BlackBerry Docs	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 Router und/oder Proxyserver	Standardmäßig stellt BlackBerry UEM eine direkte Verbindung mit der BlackBerry Infrastructure über die Ports 3101 und 443 her. Wenn die Sicherheitsrichtlinie Ihres Unternehmens jedoch vorschreibt, dass interne Systeme keine direkten Verbindungen mit dem Internet herstellen dürfen, können Sie den BlackBerry Router oder einen TCP-Proxyserver eines Drittanbieters installieren, der SOCKs v5 ohne Authentifizierung unterstützt. Der BlackBerry UEM Core und BlackBerry Proxy unterstützen das Herstellen von Verbindungen mit dem BlackBerry Dynamics NOC über den HTTP-Proxyserver eines Drittanbieters.
BlackBerry Infrastructure und BlackBerry Dynamics NOC	Die BlackBerry Infrastructure registriert Benutzerinformationen für die Geräteaktivierung, überprüft Lizenzinformationen für BlackBerry UEM und stellt einen vertrauenswürdigen Pfad, der auf einer starken, kryptografischen gegenseitigen Authentifizierung basiert, zwischen dem Unternehmen und jedem Benutzer bereit. Das BlackBerry Dynamics NOC ist ein räumlich getrenntes NOC, das eine sichere Kommunikation zwischen den BlackBerry Dynamics-Apps auf Geräten und den BlackBerry UEM Core, BlackBerry Proxy sowie BlackBerry Enterprise Mobility Server ermöglicht.

Verteilte Installation von BlackBerry UEM

Dieses Diagramm zeigt, wie die BlackBerry UEM-Komponenten miteinander verbunden sind, wenn der BlackBerry Connectivity Node und die Benutzerschnittstelle getrennt von den primären BlackBerry UEM-Komponenten installiert werden.



Weitere Informationen zu den für Verbindungen zwischen den Komponenten verwendeten Ports finden Sie in der Dokumentation zur Planung unter „Konfigurieren von Ports“.

Komponentenname	Beschreibung
Primäre BlackBerry UEM-Komponenten	Die primären BlackBerry UEM-Komponenten beinhalten den BlackBerry UEM Core und alle Komponenten, die mit ihm auf demselben Server installiert werden.
BlackBerry UEM Core	BlackBerry UEM Core ist die zentrale Komponente der BlackBerry UEM-Architektur. Er weist mehrere Unterkomponenten auf, die verantwortlich sind für: • Protokollierung, Überwachung, Reporting und Verwaltungsfunktionen • Authentifizierungs- und Autorisierungsdienste • Planen und Senden von Befehlen, IT-Richtlinien und Profilen an Geräte • Sendet Benutzer-, Richtlinien- und andere Konfigurationsdaten an die auf Geräten installierten BlackBerry Dynamics-Apps.

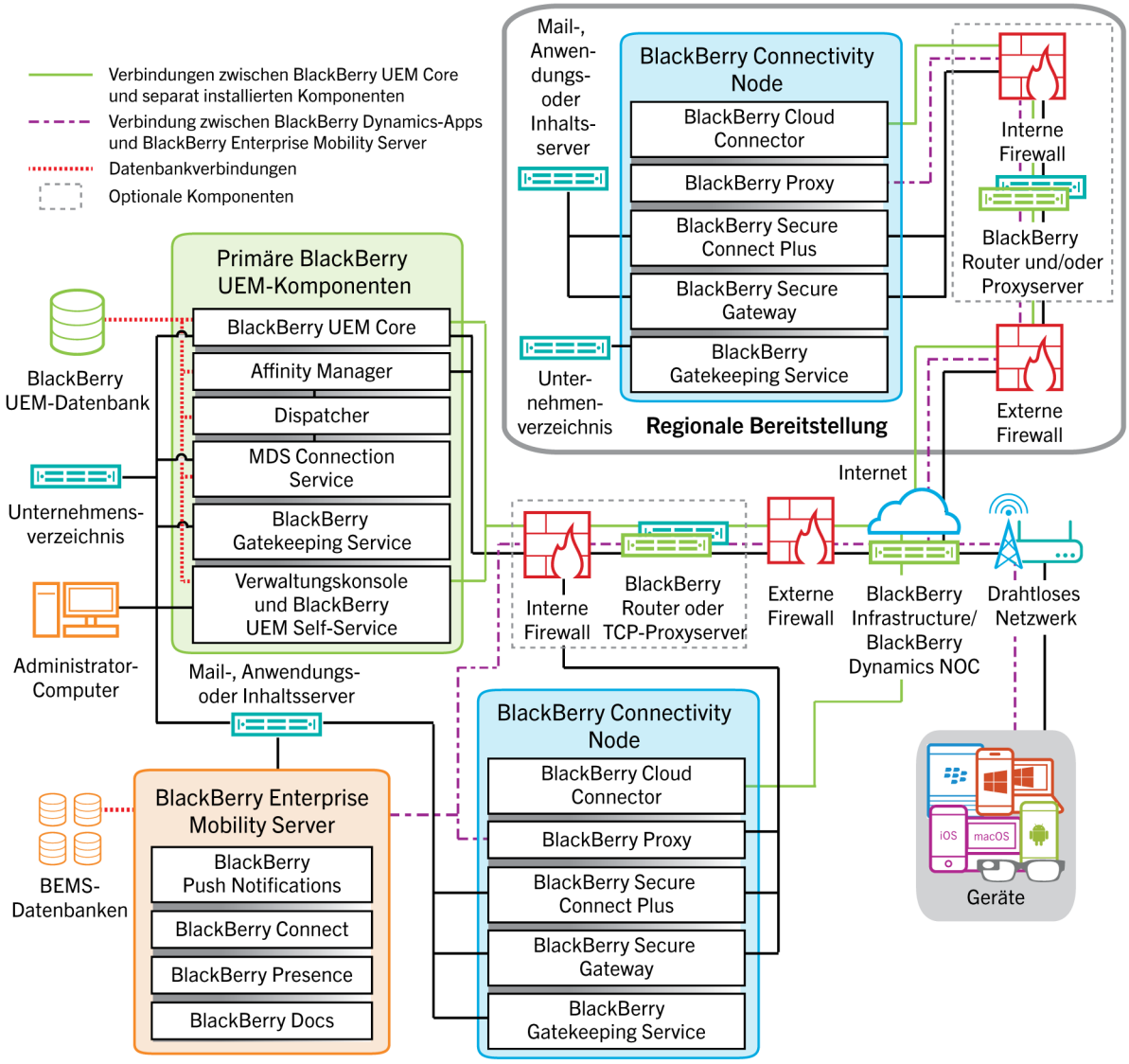
Komponentenname	Beschreibung
BlackBerry UEM-Datenbank	Die BlackBerry UEM-Datenbank ist eine relationale Datenbank, die Informationen zum Benutzerkonto und der Konfiguration enthält, die von BlackBerry UEM für die Verwaltung von Geräten und BlackBerry Dynamics-Apps verwendet werden.
BlackBerry MDS Connection Service	Der BlackBerry MDS Connection Service stellt eine sichere Verbindung zwischen BlackBerry 10-Geräten und dem Netzwerk Ihres Unternehmens bereit, wenn das Gerät nicht mit Ihrem Wi-Fi-Geschäftsnetzwerk verbunden ist oder eine VPN-Verbindung verwendet.
BlackBerry Dispatcher	Der BlackBerry Dispatcher stellt sichere Konnektivität unter Verwendung von IPPP für BlackBerry 10-Geräte bereit.
BlackBerry Affinity Manager	Der BlackBerry Affinity Manager ist für die Aufrechterhaltung einer aktiven SRP-Verbindung zwischen BlackBerry 10-Geräten und der BlackBerry Infrastructure verantwortlich, wenn diese Geräte BlackBerry Secure Connect Plus nicht verwenden.
BlackBerry Gatekeeping Service (primär)	Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf BlackBerry UEM 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.
Remote-UI-Komponenten	Die Verwaltungskonsole und BlackBerry UEM Self-Service können separat von anderen BlackBerry UEM-Komponenten installiert werden. Wenn Sie sie separat installieren, wird auch eine BlackBerry Management Console Core-Instanz installiert.
BlackBerry Management Console Core	Der BlackBerry Management Console Core verarbeitet Unteraufgaben, die für administrative Aktivitäten spezifisch sind.
Verwaltungskonsole und BlackBerry UEM Self-Service	Die Verwaltungskonsole und der BlackBerry UEM Self-Service bilden eine webbasierte Konsole, die Administrator- und Benutzerzugriff auf BlackBerry UEM ermöglicht. Sie können separat von anderen BlackBerry UEM-Komponenten installiert werden. Sie können Systemeinstellungen, Benutzer, Geräte und Apps über die Verwaltungskonsole verwalten. Benutzer können auf den BlackBerry UEM Self-Service zugreifen, um ein Aktivierungskennwort einzurichten und Befehle, z. B. zum Einrichten des Kennworts, Sperren des Geräts und Löschen von Gerätedaten, an Geräte zu senden.

Komponentenname	Beschreibung
BlackBerry Connectivity Node	Der BlackBerry Connectivity Node installiert Instanzen der BlackBerry UEM-Geräteverbindungskomponenten, die eine Verbindung mit der Domäne Ihres Unternehmens herstellen, auf einem anderen Server als der BlackBerry UEM Core. Jeder BlackBerry Connectivity Node beinhaltet die folgenden Komponenten: • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service
BlackBerry Cloud Connector	Der BlackBerry Cloud Connector ermöglicht die Kommunikation der BlackBerry Connectivity Node-Komponenten mit dem BlackBerry UEM Core. Die Kommunikation zwischen dem BlackBerry Cloud Connector und BlackBerry UEM Core erfolgt über die BlackBerry Infrastructure.
BlackBerry Proxy	Der BlackBerry Proxy sorgt für eine sichere Verbindung zwischen Ihrem Unternehmen und dem BlackBerry Dynamics NOC. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen des BlackBerry Dynamics NOC ermöglicht.
BlackBerry Secure Connect Plus	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.
BlackBerry Secure Gateway	Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum E-Mail-Server Ihres Unternehmens für iOS-Geräte.
BlackBerry Gatekeeping Service (BlackBerry Connectivity Node)	BlackBerry UEM kann Instanzen des BlackBerry Gatekeeping Service, die mit dem BlackBerry Connectivity Node installiert werden, für die Verwaltung von Gatekeeping auf Ihrem E-Mail-Server verwenden. Jede Instanz muss in der Lage sein, auf den Gatekeeping-Server Ihres Unternehmens zuzugreifen. Wenn Gatekeeping-Daten nur von dem BlackBerry Gatekeeping Service verwaltet werden sollen, der mit den primären BlackBerry UEM-Komponenten installiert ist, können Sie die BlackBerry Gatekeeping Service in jedem BlackBerry Connectivity Node deaktivieren.
BlackBerry Enterprise Mobility Server	BEMS führt verschiedene Dienste zusammen, die zum Senden und Empfangen von Daten von BlackBerry Dynamics-Apps verwendet werden, z. B. BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence und BlackBerry Docs.
BlackBerry Enterprise Mobility Server-Datenbanken	In den BEMS-Datenbanken werden Benutzer-, App-, Richtlinien- und Konfigurationsinformationen gespeichert.

Komponentenname	Beschreibung
BlackBerry Infrastructure und BlackBerry Dynamics NOC	Die BlackBerry Infrastructure registriert Benutzerinformationen für die Geräteaktivierung, überprüft Lizenzinformationen für BlackBerry UEM und stellt einen vertrauenswürdigen Pfad, der auf einer starken, kryptografischen gegenseitigen Authentifizierung basiert, zwischen dem Unternehmen und jedem Benutzer bereit. Das BlackBerry Dynamics NOC ist ein räumlich getrenntes NOC, das eine sichere Kommunikation zwischen den BlackBerry Dynamics-Apps auf Geräten und BlackBerry UEM Core, BlackBerry Proxy sowie BlackBerry Enterprise Mobility Server ermöglicht.

Regionale Bereitstellung von BlackBerry UEM

Dieses Diagramm zeigt, wie die BlackBerry UEM-Komponenten miteinander verbunden sind, wenn Instanzen von BlackBerry Connectivity Node an unterschiedlichen Standorten installiert werden. Sie können Servergruppen verwenden, um die regionale Instanz von BlackBerry Connectivity Node anzugeben, mit der sich ein Gerät verbindet.



Weitere Informationen zu den für Verbindungen zwischen den Komponenten verwendeten Ports finden Sie in der Dokumentation zur Planung unter „Konfigurieren von Ports“.

Komponentenname	Beschreibung
Primäre BlackBerry UEM-Komponenten	Die primären BlackBerry UEM-Komponenten beinhalten den BlackBerry UEM Core und alle Komponenten, die mit ihm auf demselben Server installiert werden.

Komponentenname	Beschreibung
BlackBerry UEM Core	BlackBerry UEM Core ist die zentrale Komponente der BlackBerry UEM-Architektur. Er weist mehrere Unterkomponenten auf, die verantwortlich sind für: • Protokollierung, Überwachung, Reporting und Verwaltungsfunktionen • Authentifizierungs- und Autorisierungsdienste • Planen und Senden von Befehlen, IT-Richtlinien und Profilen an Geräte • Sendet Benutzer-, Richtlinien- und andere Konfigurationsdaten an die auf Geräten installierten BlackBerry Dynamics-Apps.
BlackBerry UEM-Datenbank	Die BlackBerry UEM-Datenbank ist eine relationale Datenbank, die Informationen zum Benutzerkonto und der Konfiguration enthält, die von BlackBerry UEM für die Verwaltung von Geräten und BlackBerry Dynamics-Apps verwendet werden.
BlackBerry MDS Connection Service	Der BlackBerry MDS Connection Service stellt eine sichere Verbindung zwischen BlackBerry 10-Geräten und dem Netzwerk Ihres Unternehmens bereit, wenn das Gerät nicht mit Ihrem Wi-Fi-Geschäftsnetzwerk verbunden ist oder eine VPN-Verbindung verwendet.
BlackBerry Dispatcher	Der BlackBerry Dispatcher stellt sichere Konnektivität unter Verwendung von IPPP für BlackBerry 10-Geräte bereit.
BlackBerry Affinity Manager	Der BlackBerry Affinity Manager ist für die Aufrechterhaltung einer aktiven SRP-Verbindung zwischen BlackBerry 10-Geräten und der BlackBerry Infrastructure verantwortlich, wenn diese Geräte BlackBerry Secure Connect Plus nicht verwenden.
BlackBerry Gatekeeping Service (primär)	Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf BlackBerry UEM 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.
Verwaltungskonsole und BlackBerry UEM Self-Service	Die Verwaltungskonsole und der BlackBerry UEM Self-Service bilden eine webbasierte Konsole, die Administrator- und Benutzerzugriff auf BlackBerry UEM ermöglicht. Sie können separat von anderen BlackBerry UEM-Komponenten installiert werden. Sie können Systemeinstellungen, Benutzer, Geräte und Apps über die Verwaltungskonsole verwalten. Benutzer können auf den BlackBerry UEM Self-Service zugreifen, um ein Aktivierungskennwort einzurichten und Befehle, z. B. zum Einrichten des Kennworts, Sperren des Geräts und Löschen von Gerätedaten, an Geräte zu senden.

Komponentenname	Beschreibung
BlackBerry Connectivity Node	Der BlackBerry Connectivity Node installiert Instanzen der BlackBerry UEM-Geräteverbindungskomponenten, die eine Verbindung mit der Domäne Ihres Unternehmens herstellen, auf einem anderen Server als der BlackBerry UEM Core. Jeder BlackBerry Connectivity Node beinhaltet die folgenden Komponenten: • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service Bei regionalen Bereitstellungen von BlackBerry Connectivity Node müssen Sie die Verbindung zwischen BlackBerry UEM Core und der Servergruppe konfigurieren, die den regionalen BlackBerry Connectivity Node beinhaltet.
BlackBerry Cloud Connector	Der BlackBerry Cloud Connector ermöglicht die Kommunikation der BlackBerry Connectivity Node-Komponenten mit dem BlackBerry UEM Core. Die Kommunikation zwischen dem BlackBerry Cloud Connector und BlackBerry UEM Core erfolgt über die BlackBerry Infrastructure.
BlackBerry Proxy	Der BlackBerry Proxy sorgt für eine sichere Verbindung zwischen Ihrem Unternehmen und dem BlackBerry Dynamics NOC. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen des BlackBerry Dynamics NOC ermöglicht.
BlackBerry Secure Connect Plus	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.
BlackBerry Secure Gateway	Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry UEM zum E-Mail-Server Ihres Unternehmens für iOS-Geräte.
BlackBerry Gatekeeping Service (BlackBerry Connectivity Node)	BlackBerry UEM kann Instanzen des BlackBerry Gatekeeping Service, die mit dem BlackBerry Connectivity Node installiert werden, für die Verwaltung von Gatekeeping auf Ihrem E-Mail-Server verwenden. Jede Instanz muss in der Lage sein, auf den Gatekeeping-Server Ihres Unternehmens zuzugreifen. Wenn Gatekeeping-Daten nur von dem BlackBerry Gatekeeping Service verwaltet werden sollen, der mit den primären BlackBerry UEM-Komponenten installiert ist, können Sie die BlackBerry Gatekeeping Service in jedem BlackBerry Connectivity Node deaktivieren.
BlackBerry Enterprise Mobility Server	BEMS führt verschiedene Dienste zusammen, die zum Senden und Empfangen von Daten von BlackBerry Dynamics-Apps verwendet werden, z. B. BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence und BlackBerry Docs.
BlackBerry Enterprise Mobility Server-Datenbanken	In den BEMS-Datenbanken werden Benutzer-, App-, Richtlinien- und Konfigurationsinformationen gespeichert.

Komponentenname	Beschreibung
BlackBerry Infrastructure und BlackBerry Dynamics NOC	Die BlackBerry Infrastructure registriert Benutzerinformationen für die Geräteaktivierung, überprüft Lizenzinformationen für BlackBerry UEM und stellt einen vertrauenswürdigen Pfad, der auf einer starken, kryptografischen gegenseitigen Authentifizierung basiert, zwischen dem Unternehmen und jedem Benutzer bereit. Das BlackBerry Dynamics NOC ist ein räumlich getrenntes NOC, das eine sichere Kommunikation zwischen den BlackBerry Dynamics-Apps auf Geräten und den BlackBerry UEM Core, BlackBerry Proxy sowie BlackBerry Enterprise Mobility Server ermöglicht.

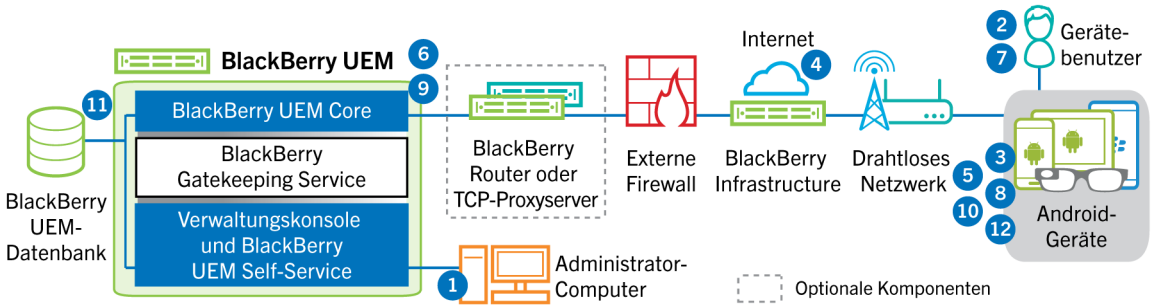
Aktivieren von Geräten und BlackBerry Dynamics-Apps

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 für BlackBerry Dynamics-Apps" in der Dokumentation für Administratoren.

Datenfluss: Aktivieren eines Android Enterprise Geschäftlich und persönlich – Benutzer-Datenschutz-Geräts mit einem verwalteten Google Play-Konto



Dieser Datenfluss gilt, wenn Sie zulassen, dass BlackBerry UEM Google Play-Konten verwaltet. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

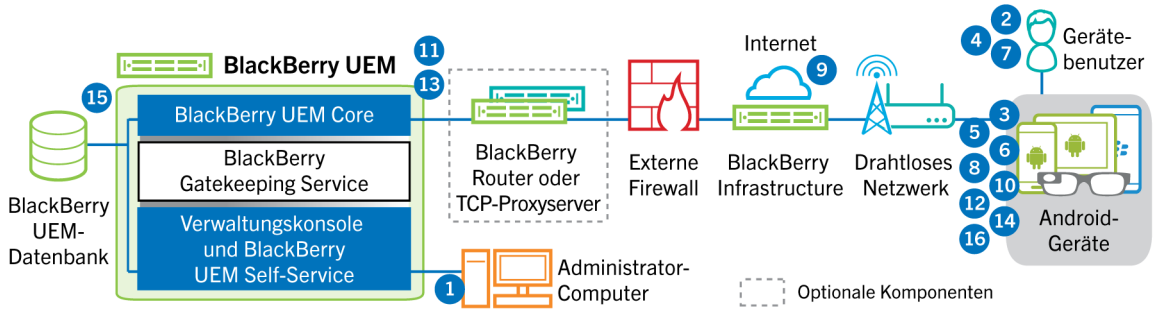
1. Führen Sie die folgenden Schritte aus:
   a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
   b. Stellen Sie sicher, dass die Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“ dem Benutzer zugewiesen ist.
   c. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
      - Automatisches Generieren eines Geräteaktivierungskennworts und optional eines QR Code s, und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer

- Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzername und Kennwort 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 und ein QR Code anzeigen kann

2. Der Benutzer lädt den BlackBerry UEM Client aus Google Play herunter und installiert ihn auf dem Gerät. Nach der Installation öffnet der Benutzer den BlackBerry UEM Client und gibt seine E-Mail-Adresse und das Aktivierungskennwort ein oder scannt den QR Code.
3. Der BlackBerry UEM Client auf dem Gerät führt folgende Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
4. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Adresse für den Benutzer ab
   c. Sendet die Adresse an den BlackBerry UEM Client
5. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
6. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Bestimmt die Aktivierungsart, die dem Benutzerkonto zugewiesen ist
   b. Stellt eine Verbindung zu Google her und erstellt einen verwalteten Google Play-Benutzer
   c. Erstellen eines Gerätekennworts
   d. Verknüpft die Geräteinstanz mit dem angegebenen Benutzerkonto
   e. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   f. Sendet die verwalteten Google Play-Kontodaten des Benutzers und eine Nachricht über die erfolgreiche Authentifizierung an das Gerät
7. Wenn das Gerät nicht verschlüsselt ist, wird der Benutzer dazu aufgefordert, es zu verschlüsseln.
8. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Stellt zur Überprüfung des Benutzers eine Verbindung mit Google her
   b. Erstellt das Arbeitsprofil auf dem Gerät
   c. Erstellt eine CSR mithilfe der von BlackBerry UEM empfangenen Informationen und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.
9. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
   b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
   c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

   Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.
10. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
11. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet die angeforderten Konfigurationsinformationen an das Gerät.
12. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Android Enterprise Geschäftlich und persönlich – vollständige Kontrolle-Geräts mit einem verwalteten Google Play-Konto



Dieser Datenfluss gilt, wenn Sie zulassen, dass BlackBerry UEM Google Play-Konten verwaltet. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

1. Führen Sie die folgenden Schritte aus:
   a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
   b. Stellen Sie sicher, dass die Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle“ dem Benutzer zugewiesen ist.
   c. Richten Sie das Aktivierungskennwort für den Benutzer ein.
2. Der Benutzer setzt sein Gerät auf die werkseitigen Standardeinstellungen zurück.
3. Das Gerät wird neu gestartet und fordert den Benutzer dazu auf, ein Wi-Fi-Netzwerk auszuwählen und ein Konto hinzuzufügen.
4. Der Benutzer gibt `afw#blackberry` anstelle seines Google-Benutzernamens ein.
5. Das Gerät führt die folgenden Aktionen aus:
   a. Fordert den Benutzer auf, das Gerät zu entschlüsseln und startet neu
   b. Lädt den BlackBerry UEM Client aus Google Play herunter und installiert ihn.
6. Der BlackBerry UEM Client auf dem Gerät fordert den Benutzer dazu auf, seine E-Mail-Adresse und sein Aktivierungskennwort einzugeben.
7. Der Benutzer gibt seine E-Mail-Adresse und sein Aktivierungskennwort ein oder scannt den QR Code.
8. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
9. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Serveradresse für den Benutzer ab
   c. Sendet die Serveradresse an den BlackBerry UEM Client
10. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
11. BlackBerry UEM führt die folgenden Aktionen aus:
    a. Bestimmt die Aktivierungsart, die dem Benutzerkonto zugewiesen ist
    b. Stellt eine Verbindung zu Google her und erstellt einen verwalteten Google Play-Benutzer

c. Erstellen eines Gerätekennworts
d. Verknüpft die Geräteinstanz mit dem angegebenen Benutzerkonto
e. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
f. Sendet die verwalteten Google Play-Kontodaten des Benutzers und eine Nachricht über die erfolgreiche Authentifizierung an das Gerät

12. Die BlackBerry UEM Client führt die folgenden Aktionen aus:

a. Stellt zur Überprüfung des Benutzers eine Verbindung mit Google her
b. Erstellt das Arbeitsprofil auf dem Gerät
c. Erstellt eine CSR mithilfe der von BlackBerry UEM empfangenen Informationen und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.

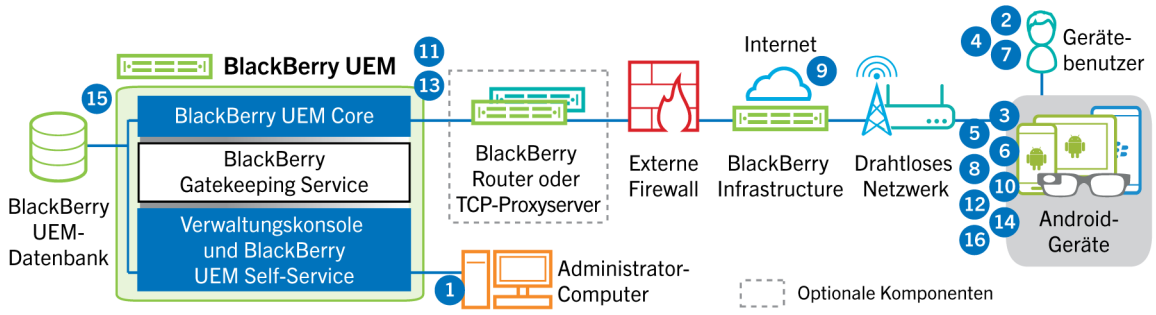
13. BlackBerry UEM führt die folgenden Aktionen aus:

a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.

14. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
15. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet die angeforderten Konfigurationsinformationen an das Gerät.
16. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Android Enterprise Nur geschäftlicher Bereich-Geräts mit einem verwalteten Google Play-Konto



Dieser Datenfluss gilt, wenn Sie zulassen, dass BlackBerry UEM Google Play-Konten verwaltet. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

1. Führen Sie die folgenden Schritte aus:

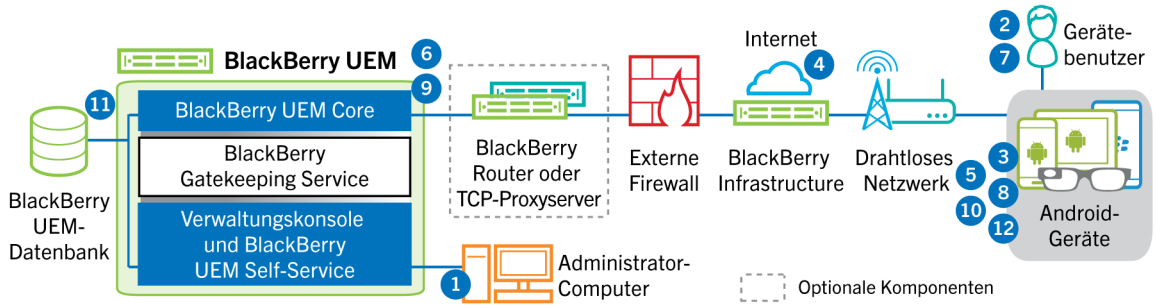
a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
b. Stellen Sie sicher, dass die Aktivierungsart „Nur geschäftlicher Bereich“ dem Benutzer zugewiesen ist.
c. Richten Sie das Aktivierungskennwort für den Benutzer ein.

2. Der Benutzer setzt sein Gerät auf die werkseitigen Standardeinstellungen zurück.
3. Das Gerät wird neu gestartet und fordert den Benutzer dazu auf, ein Wi-Fi-Netzwerk auszuwählen und ein Konto hinzuzufügen.

4. Der Benutzer gibt `afw#blackberry` anstelle seines Google-Benutzernamens ein.
5. Das Gerät führt die folgenden Aktionen aus:
   a. Wenn das Gerät nicht verschlüsselt ist, fordert es den Benutzer auf, das Gerät zu verschlüsseln und neu zu starten.
   b. Lädt den BlackBerry UEM Client aus Google Play herunter und installiert ihn.
6. Der BlackBerry UEM Client auf dem Gerät fordert den Benutzer dazu auf, seine E-Mail-Adresse und sein Aktivierungskennwort einzugeben.
7. Der Benutzer gibt seine E-Mail-Adresse und sein Aktivierungskennwort ein oder scannt den QR Code.
8. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
9. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Serveradresse für den Benutzer ab
   c. Sendet die Serveradresse an den BlackBerry UEM Client
10. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
11. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Bestimmt die Aktivierungsart, die dem Benutzerkonto zugewiesen ist
   b. Stellt eine Verbindung zu Google her und erstellt einen verwalteten Google Play-Benutzer
   c. Erstellen eines Gerätekennworts
   d. Verknüpft die Geräteinstanz mit dem angegebenen Benutzerkonto
   e. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   f. Sendet die verwalteten Google Play-Kontodaten des Benutzers und eine Nachricht über die erfolgreiche Authentifizierung an das Gerät
12. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Stellt zur Überprüfung des Benutzers eine Verbindung mit Google her
   b. Erstellt eine CSR mithilfe der von BlackBerry UEM empfangenen Informationen und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.
13. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
   b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
   c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

   Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.
14. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
15. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet die angeforderten Konfigurationsinformationen an das Gerät.
16. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Android Enterprise Geschäftlich und persönlich – Benutzer-Datenschutz-Geräts in einer Google-Domäne



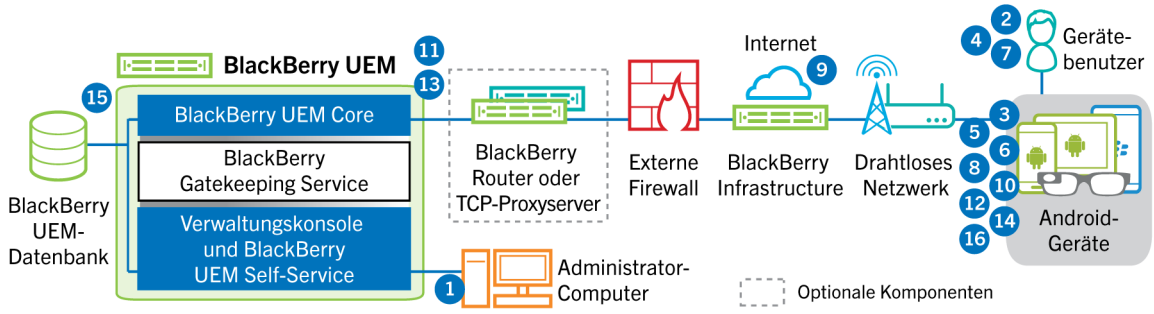
Dieser Datenfluss findet Anwendung, wenn BlackBerry UEM mit einer Google Cloud- oder G Suite-Domäne verbunden ist. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

1. Führen Sie die folgenden Schritte aus:
   a. Stellen Sie sicher, dass der Benutzer über ein Google-Konto verfügt, das mit der geschäftlichen E-Mail-Adresse des Endanwenders verknüpft ist. Optional können Sie während des Aktivierungsprozesses BlackBerry UEM zum Erstellen des Google-Kontos für den Benutzer konfigurieren. Wenn BlackBerry UEM das Konto für den Benutzer in Google erstellt, erhält der Benutzer eine E-Mail aus der Google-Domain mit dem Kennwort zu seinem Google-Konto.
   b. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis. Verwenden Sie bei der Angabe der E-Mail-Adresse die E-Mail-Adresse, die mit dem Google-Konto des Benutzers verknüpft ist.
   c. Stellen Sie sicher, dass die Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“ dem Benutzer zugewiesen ist.
   d. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
      - Automatisches Generieren eines Geräteaktivierungskennworts und optional eines QR Code s, und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer
      - Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzername und Kennwort 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 und ein QR Code anzeigen kann
2. Der Benutzer lädt den BlackBerry UEM Client aus Google Play herunter und installiert ihn auf dem Gerät. Nach der Installation öffnet der Benutzer den BlackBerry UEM Client und gibt seine E-Mail-Adresse und das Aktivierungskennwort ein oder scannt den QR Code.
3. Der BlackBerry UEM Client auf dem Gerät führt folgende Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
4. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Adresse für den Benutzer ab
   c. Sendet die Adresse an den BlackBerry UEM Client
5. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.

6. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Bestimmt die Aktivierungsart, die dem Benutzerkonto zugewiesen ist
   b. Stellt eine Verbindung zur verwalteten Google-Domäne her, um die Angaben des Benutzers zu überprüfen. Wenn der Benutzer nicht vorhanden ist, kann BlackBerry UEM je nach Konfiguration den Benutzer in der Google-Domäne erstellen.
   c. Erstellen eines Gerätekennworts
   d. Verknüpft die Geräteinstanz mit dem angegebenen Benutzerkonto
   e. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   f. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät
7. Wenn das Gerät nicht verschlüsselt ist, wird der Benutzer dazu aufgefordert, es zu verschlüsseln.
8. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Erstellt das Arbeitsprofil auf dem Gerät
   b. Fordert den Benutzer zur Angabe der Google-Kontoinformationen des Benutzers auf
   c. Stellt eine Verbindung zur verwalteten Google-Domäne her, um den Benutzer zu authentifizieren
   d. Erstellt das Arbeitsprofil auf dem Gerät
   e. Erstellt eine CSR mithilfe der von BlackBerry UEM empfangenen Informationen und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.
9. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
   b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
   c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

   Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.
10. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
11. BlackBerry UEM speichert die Geräteinformationen und sendet die angeforderten Konfigurationsinformationen an das Gerät.
12. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Android Enterprise Geschäftlich und persönlich – vollständige Kontrolle-Geräts in einer Google-Domäne



Dieser Datenfluss findet Anwendung, wenn BlackBerry UEM mit einer Google Cloud- oder G Suite-Domäne verbunden ist. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

1. Führen Sie die folgenden Schritte aus:

   a. Stellen Sie sicher, dass der Benutzer über ein Google-Konto verfügt, das mit der geschäftlichen E-Mail-Adresse des Endanwenders verknüpft ist. Optional können Sie während des Aktivierungsprozesses BlackBerry UEM zum Erstellen des Google-Kontos für den Benutzer konfigurieren. Wenn BlackBerry UEM das Konto für den Benutzer in Google erstellt, erhält der Benutzer eine E-Mail aus der Google-Domain mit dem Kennwort zu seinem Google-Konto.
   b. Stellen Sie sicher, dass die Einstellung „EMM-Richtlinie erzwingen“ für die Google-Domäne aktiviert ist. Diese Einstellung legt fest, dass aktivierte Geräte von einem EMM-Provider, wie z. B. BlackBerry UEM, verwaltet werden.
   c. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis. Verwenden Sie bei der Angabe der E-Mail-Adresse die E-Mail-Adresse, die mit dem Google-Konto des Benutzers verknüpft ist.
   d. Stellen Sie sicher, dass die Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle“ dem Benutzer zugewiesen ist.
   e. Richten Sie das Aktivierungskennwort für den Benutzer ein.
2. Der Benutzer setzt sein Gerät auf die werkseitigen Standardeinstellungen zurück.
3. Das Gerät wird neu gestartet und fordert den Benutzer dazu auf, ein Wi-Fi-Netzwerk auszuwählen und ein Konto hinzuzufügen.
4. Der Benutzer gibt seine geschäftliche E-Mail-Adresse und das Kennwort ein.
5. Das Gerät kommuniziert mit der Google-Domäne, um festzustellen, ob es sich um einen geschäftlichen Benutzer handelt, und zu überprüfen, ob die Einstellung für die Durchsetzung der EMM-Richtlinie aktiviert ist. Nachdem das Gerät die entsprechenden Validierungen durchgeführt hat, führt es die folgenden Aktionen aus:
   a. Wenn das Gerät nicht verschlüsselt ist, fordert es den Benutzer auf, das Gerät zu verschlüsseln und neu zu starten.
   b. Lädt den BlackBerry UEM Client aus Google Play herunter und installiert ihn.
6. Der BlackBerry UEM Client auf dem Gerät fordert den Benutzer dazu auf, seine E-Mail-Adresse und sein Aktivierungskennwort einzugeben.
7. Der Benutzer gibt seine E-Mail-Adresse und sein Aktivierungskennwort ein oder scannt den QR Code.
8. Der BlackBerry UEM Client auf dem Gerät führt folgende Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
9. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Serveradresse für den Benutzer ab
   c. Sendet die Serveradresse an den BlackBerry UEM Client
10. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
11. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Bestimmt die Aktivierungsart, die dem Benutzerkonto zugewiesen ist
   b. Stellt eine Verbindung zur Google-Domäne her, um die Angaben des Benutzers zu überprüfen. Wenn der Benutzer nicht vorhanden ist, kann BlackBerry UEM je nach Konfiguration den Benutzer in der Google-Domäne erstellen
   c. Erstellen eines Gerätekennworts
   d. Verknüpft die Geräteinstanz mit dem angegebenen Benutzerkonto
   e. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   f. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät
12. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Erstellt das Arbeitsprofil auf dem Gerät

b. Fordert den Benutzer zur Angabe der Google-Kontoinformationen des Benutzers auf
c. Stellt eine Verbindung zur Google-Domäne her, um den Benutzer zu authentifizieren
d. Erstellt eine CSR mithilfe der von BlackBerry UEM empfangenen Informationen und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.

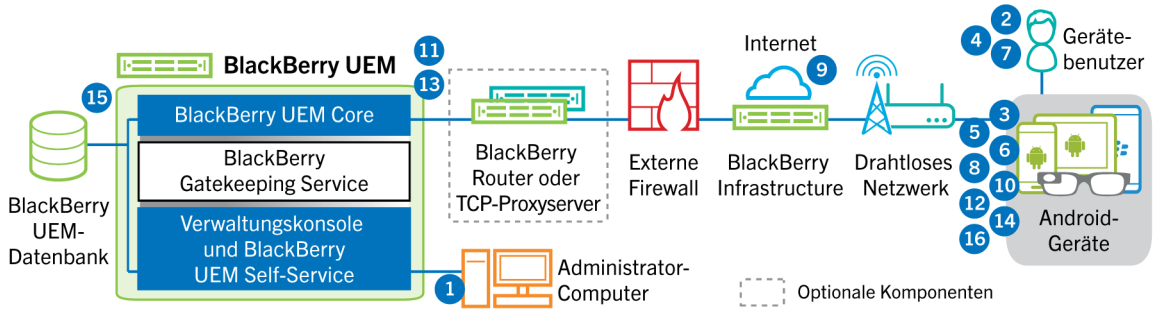
13. BlackBerry UEM führt die folgenden Aktionen aus:

a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.

14. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
15. BlackBerry UEM speichert die Geräteinformationen und sendet die angeforderten Konfigurationsinformationen an das Gerät.
16. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Android Enterprise Nur geschäftlicher Bereich-Geräts in einer Google-Domäne



Dieser Datenfluss findet Anwendung, wenn BlackBerry UEM mit einer Google Cloud- oder G Suite-Domäne verbunden ist. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

1. Führen Sie die folgenden Schritte aus:

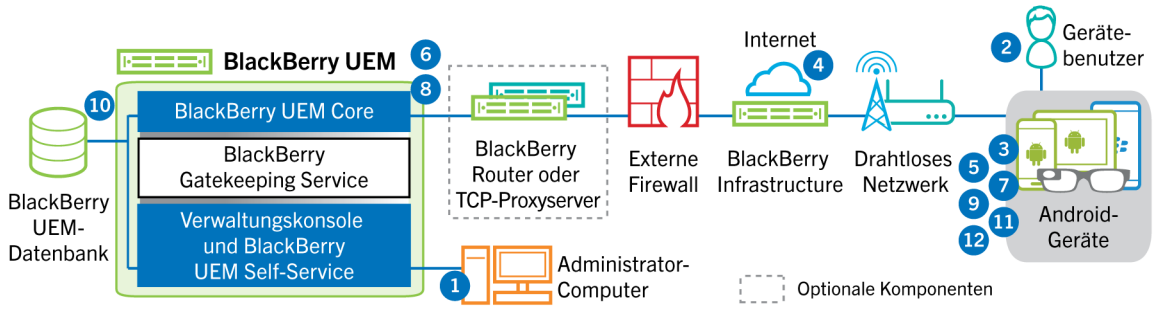
a. Stellen Sie sicher, dass der Benutzer über ein Google-Konto verfügt, das mit der geschäftlichen E-Mail-Adresse des Endanwenders verknüpft ist. Optional können Sie während des Aktivierungsprozesses BlackBerry UEM zum Erstellen des Google-Kontos für den Benutzer konfigurieren. Wenn BlackBerry UEM das Konto für den Benutzer in Google erstellt, erhält der Benutzer eine E-Mail aus der Google-Domain mit dem Kennwort zu seinem Google-Konto.
b. Stellen Sie sicher, dass die Einstellung „EMM-Richtlinie erzwingen“ für die Google-Domäne aktiviert ist. Diese Einstellung legt fest, dass aktivierte Geräte von einem EMM-Provider, wie z. B. BlackBerry UEM, verwaltet werden.
c. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis. Verwenden Sie bei der Angabe der E-Mail-Adresse die E-Mail-Adresse, die mit dem Google-Konto des Benutzers verknüpft ist.
d. Stellen Sie sicher, dass die Aktivierungsart „Nur geschäftlicher Bereich“ dem Benutzer zugewiesen ist.
e. Richten Sie das Aktivierungskennwort für den Benutzer ein.

2. Der Benutzer setzt sein Gerät auf die werkseitigen Standardeinstellungen zurück.
3. Das Gerät wird neu gestartet und fordert den Benutzer dazu auf, ein Wi-Fi-Netzwerk auszuwählen und ein Konto hinzuzufügen.
4. Der Benutzer gibt seine geschäftliche E-Mail-Adresse und das Kennwort ein.
5. Das Gerät kommuniziert mit der Google-Domäne, um festzustellen, ob es sich um einen geschäftlichen Benutzer handelt, und zu überprüfen, ob die Einstellung für die Durchsetzung der EMM-Richtlinie aktiviert ist. Nachdem das Gerät die entsprechenden Validierungen durchgeführt hat, führt es die folgenden Aktionen aus:
   a. Wenn das Gerät nicht verschlüsselt ist, fordert es den Benutzer auf, das Gerät zu verschlüsseln und neu zu starten.
   b. Lädt den BlackBerry UEM Client aus Google Play herunter und installiert ihn.
6. Der BlackBerry UEM Client auf dem Gerät fordert den Benutzer dazu auf, seine E-Mail-Adresse und sein Aktivierungskennwort einzugeben.
7. Der Benutzer gibt seine E-Mail-Adresse und sein Aktivierungskennwort ein oder scannt den QR Code.
8. Der BlackBerry UEM Client auf dem Gerät führt folgende Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
9. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Serveradresse für den Benutzer ab
   c. Sendet die Serveradresse an den BlackBerry UEM Client
10. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
11. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Bestimmt die Aktivierungsart, die dem Benutzerkonto zugewiesen ist
   b. Stellt eine Verbindung zur Google-Domäne her, um die Angaben des Benutzers zu überprüfen. Wenn der Benutzer nicht vorhanden ist, kann BlackBerry UEM je nach Konfiguration den Benutzer in der Google-Domäne erstellen.
   c. Erstellen eines Gerätekennworts
   d. Verknüpft die Geräteinstanz mit dem angegebenen Benutzerkonto
   e. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   f. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät
12. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Fordert den Benutzer zur Angabe der Google-Kontoinformationen des Benutzers auf
   b. Stellt eine Verbindung zur Google-Domäne her, um den Benutzer zu authentifizieren
   c. Erstellt eine CSR mithilfe der von BlackBerry UEM empfangenen Informationen und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.
13. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
   b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
   c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

   Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.
14. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
15. BlackBerry UEM speichert die Geräteinformationen und sendet die angeforderten Konfigurationsinformationen an das Gerät.

16. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Android-Geräts für MDM



Die Aktivierungsart MDM-Steuerelemente wird für Geräte mit Android 10 nicht mehr unterstützt. Versuche Android-Geräte ab Version 10 mit der Aktivierungsart MDM-Steuerelemente zu aktivieren, schlagen fehl. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community.

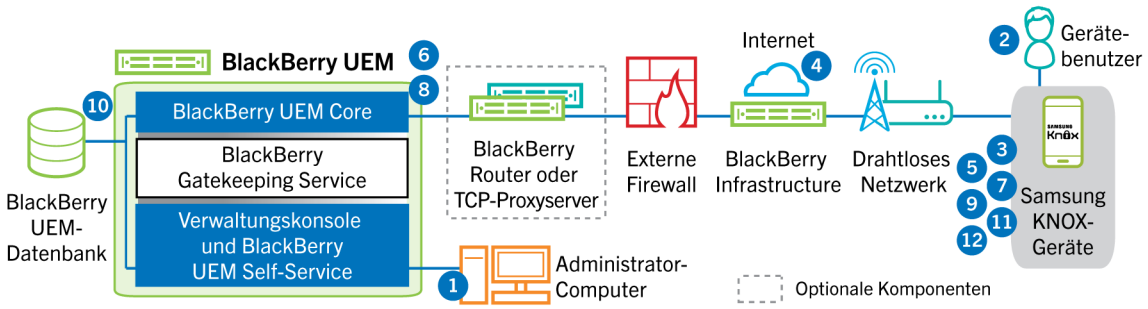
1. Führen Sie die folgenden Schritte aus:
   a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
   b. Vergewissern Sie sich, dass dem Benutzer ein Aktivierungsprofil mit der Aktivierungsart „MDM-Steuerelemente“ zugewiesen ist.
   c. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
      - Automatisches Generieren eines Geräteaktivierungskennworts und optional eines QR Code s, und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer
      - Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzername und Kennwort 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 und ein QR Code anzeigen kann
2. Der Benutzer lädt den BlackBerry UEM Client herunter und installiert ihn auf seinem Gerät. Nach der Installation öffnet der Benutzer den BlackBerry UEM Client und gibt auf dem Gerät die E-Mail-Adresse und das Aktivierungskennwort ein oder scannt den QR Code.
3. Der BlackBerry UEM Client auf dem Gerät führt folgende Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
4. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Adresse für den Benutzer ab
   c. Sendet die Adresse an den BlackBerry UEM Client
5. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
6. BlackBerry UEM führt folgende Aktionen aus:
   a. Überprüfen der Anmeldeinformationen auf Gültigkeit
   b. Erstellen eines Gerätekennworts
   c. Verknüpfen der Geräteinstanz mit dem angegebenen Benutzerkonto in der BlackBerry UEM-Datenbank
   d. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   e. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät

7. Der BlackBerry UEM Client erstellt mithilfe der von BlackBerry UEM empfangenen Informationen eine CSR-Datei und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.
8. BlackBerry UEM führt die folgenden Aktionen aus:

   a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
   b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
   c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

   Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.
9. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
10. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet die angeforderten Konfigurationsinformationen an das Gerät.
11. Der BlackBerry UEM Client überprüft, ob das Gerät Knox MDM verwendet und eine unterstützte MDM-Version ausführt. Wenn das Gerät Knox MDM verwendet, stellt das Gerät eine Verbindung zu der Samsung-Infrastruktur her und aktiviert die Knox-Verwaltungslizenz. Nachdem sie aktiviert wurde, wendet der BlackBerry UEM Client die Knox MDM IT-Richtlinienregeln von BlackBerry UEM an.
12. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Geräts für die Verwendung von Knox Workspace



1. Führen Sie die folgenden Schritte aus:
   a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
   b. Stellen Sie sicher, dass die Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)“, „Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)“ oder „Nur geschäftlicher Bereich – (Samsung Knox)“ dem Benutzer zugewiesen ist.
   c. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
      - Automatisches Generieren eines Geräteaktivierungskennworts und optional eines QR Code s, und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer
      - Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzername und Kennwort 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 und ein QR Code anzeigen kann
2. Der Benutzer lädt den BlackBerry UEM Client herunter und installiert ihn auf seinem Gerät. Nach der Installation öffnet der Benutzer den BlackBerry UEM Client und gibt auf dem Gerät die E-Mail-Adresse und das Aktivierungskennwort ein oder scannt den QR Code.
3. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
4. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Adresse für den Benutzer ab
   c. Sendet die Adresse an den BlackBerry UEM Client
5. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
6. BlackBerry UEM führt folgende Aktionen aus:
   a. Überprüfen der Anmeldeinformationen auf Gültigkeit
   b. Erstellen eines Gerätekennworts
   c. Verknüpfen der Geräteinstanz mit dem angegebenen Benutzerkonto in der BlackBerry UEM-Datenbank
   d. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   e. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät

7. Der BlackBerry UEM Client erstellt mithilfe der von BlackBerry UEM empfangenen Informationen eine CSR-Datei und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.
8. BlackBerry UEM führt die folgenden Aktionen aus:

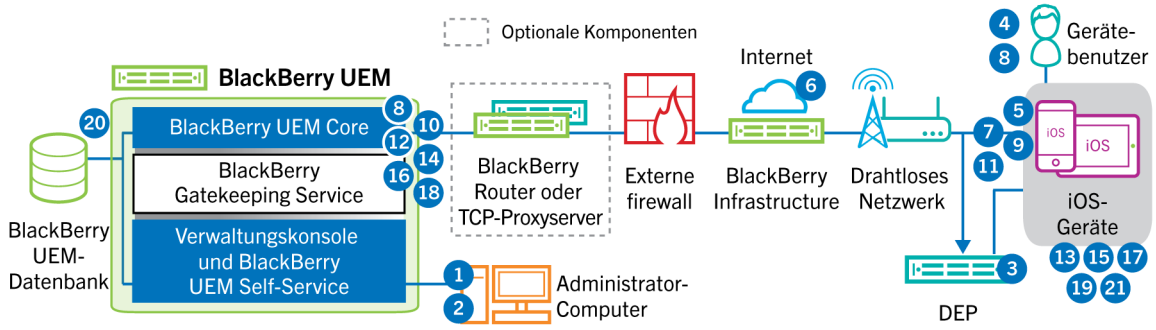
   a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
   b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
   c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

   Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.
9. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
10. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet die angeforderten Konfigurationsinformationen an das Gerät.
11. Der BlackBerry UEM Client überprüft, ob das Gerät Knox Workspace verwendet und eine unterstützte Version ausführt. Wenn das Gerät Knox Workspace verwendet, stellt das Gerät eine Verbindung zur Samsung-Infrastruktur her und aktiviert die Knox-Verwaltungslizenz. Nach der Aktivierung wendet der BlackBerry UEM Client die Knox MDM und die Knox Workspace IT-Richtlinienregeln an.
12. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Nachdem die Aktivierung abgeschlossen ist, wird der Benutzer aufgefordert, ein Kennwort für den geschäftlichen Bereich für Knox Workspace zu erstellen. Die Daten im Knox Workspace sind durch Verschlüsselung und eine Authentifizierungsmethode, wie beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt.

Hinweis: Wenn das Gerät mit der Aktivierungsart „Nur geschäftlicher Bereich - (Samsung Knox)“ aktiviert wurde, wird der persönliche Speicherplatz nach der Einrichtung von Knox Workspace entfernt.

Datenfluss: Aktivieren eines iOS-Geräts



1. Wenn Sie planen, das Programm zur Geräteregistrierung von Apple zu verwenden, führen Sie die folgenden Schritte aus:

   a. Stellen Sie sicher, dass BlackBerry UEM für die Synchronisation mit DEP konfiguriert ist.
   b. Registrieren Sie das Gerät im DEP, und weisen Sie es einem MDM Server zu.
   c. Weisen Sie dem Gerät eine Registrierungskonfiguration zu.
2. Führen Sie die folgenden Schritte aus:

   a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
   b. Weisen Sie dem Benutzer ein Aktivierungsprofil zu.
   c. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:

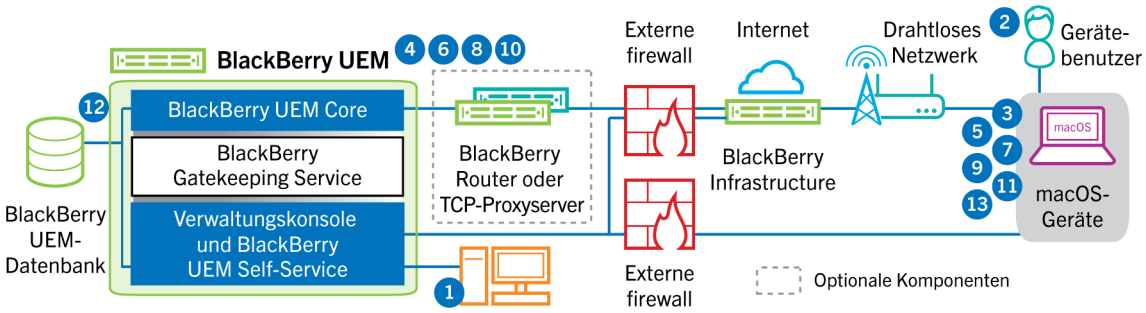
- Automatisches Generieren eines Geräteaktivierungskennworts und optional eines QR Code s, und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer
- Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzername und Kennwort direkt oder per E-Mail
- Kein Einrichten eines Geräteaktivierungskennworts und keine Mitteilung der BlackBerry UEM Self-Service-Adresse an den Benutzer, sodass der Benutzer ein eigenes Aktivierungskennwort festlegen und ein QR Code anzeigen kann

3. Wenn das Gerät im Apple DEP registriert ist, kommuniziert das Gerät mit dem Apple DEP Web Service während der Ersteinrichtung. Wenn Sie das Gerät zur Installation der BlackBerry UEM Client-App konfiguriert haben, lädt das Gerät diese automatisch herunter und installiert sie.
4. Falls das Gerät nicht beim Apple DEP registriert ist oder wenn Sie das Gerät nicht zur Installation des BlackBerry UEM Client konfiguriert haben, muss der Benutzer den BlackBerry UEM Client manuell herunterladen und auf dem Gerät installieren. Nach der Installation öffnet der Benutzer den BlackBerry UEM Client und gibt auf dem Gerät die E-Mail-Adresse und das Aktivierungskennwort ein oder scannt den QR Code.
5. Die BlackBerry UEM Client führt die folgenden Aktionen aus:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
6. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Adresse für den Benutzer ab
   c. Sendet die Adresse an den BlackBerry UEM Client
7. Der BlackBerry UEM Client stellt eine Verbindung mit BlackBerry UEM über den Aufruf „HTTP CONNECT“ über Port 443 her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
8. BlackBerry UEM führt folgende Aktionen aus:
   a. Überprüfen der Anmeldeinformationen auf Gültigkeit
   b. Erstellen eines Gerätekennworts
   c. Verknüpfen der Geräteinstanz mit dem angegebenen Benutzerkonto in der BlackBerry UEM-Datenbank
   d. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   e. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät
9. Der BlackBerry UEM Client erstellt mithilfe der von BlackBerry UEM empfangenen Informationen eine CSR und sendet eine Anforderung für ein Client-Zertifikat über HTTPS.
10. BlackBerry UEM führt die folgenden Aktionen aus:
    a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
    b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
    c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den BlackBerry UEM Client

    Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem BlackBerry UEM Client und BlackBerry UEM hergestellt.
11. Der BlackBerry UEM Client zeigt eine Nachricht an, um den Benutzer darüber zu informieren, dass ein Zertifikat zum Abschließen der Aktivierung installiert werden muss. Der Benutzer klickt auf „OK“ und wird an den Link für die Aktivierung des nativen MDM-Daemons weitergeleitet. Der BlackBerry UEM Client baut eine Verbindung mit BlackBerry UEM auf.
12. BlackBerry UEM stellt das MDM-Profil für das Gerät bereit. In diesem Profil sind die MDM-Aktivierungs-URL und die Challenge enthalten. Das MDM-Profil ist als signierte PKCS#7-Nachricht gewrappt, in der die vollständige Zertifikatskette des Signaturgebers enthalten ist, wodurch es dem Gerät möglich ist, das Profil zu überprüfen. Dadurch wird der Anmeldungsvorgang ausgelöst.
13. Der native MDM-Daemon auf dem Gerät sendet das Geräteprofil, einschließlich der Kunden-ID, der Sprache und der Version des Betriebssystems, an BlackBerry UEM.

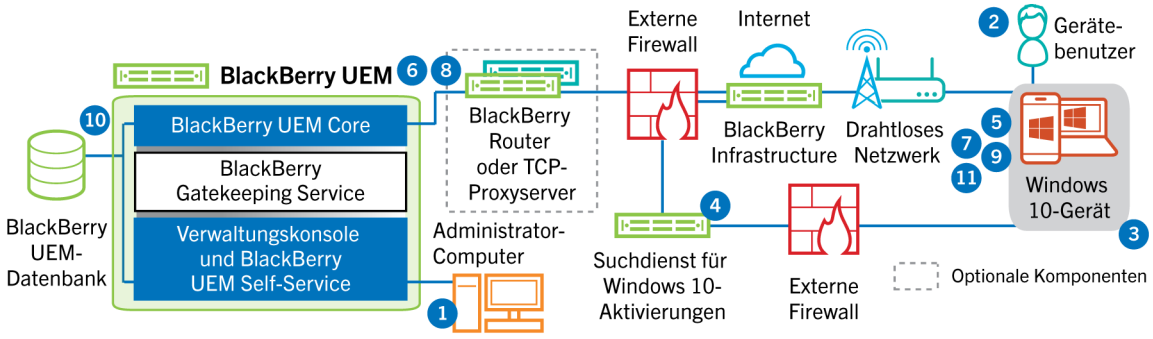
14. BlackBerry UEM überprüft, dass die Anforderung von einer Zertifizierungsstelle signiert wurde und auf den nativen MDM-Daemon mit einer erfolgreichen Authentifizierungsbenachrichtigung reagiert.
15. Der native MDM-Daemon sendet eine Anforderung an BlackBerry UEM, um ein Zertifizierungsstellenzertifikat, Funktionsinformationen der Zertifizierungsstelle und ein vom Gerät ausgegebenes Zertifikat anzufragen.
16. BlackBerry UEM sendet das Zertifizierungsstellenzertifikat, Funktionsinformationen der Zertifizierungsstelle und das vom Gerät ausgegebene Zertifikat an den nativen MDM-Daemon.
17. Der native MDM-Daemon installiert das MDM-Profil auf dem Gerät. Der BlackBerry UEM Client benachrichtigt BlackBerry UEM über die erfolgreiche Installation des MDM-Profils und des Zertifikats und fragt BlackBerry UEM periodisch ab, bis bestätigt wird, dass die MDM-Aktivierung abgeschlossen ist.
18. BlackBerry UEM bestätigt, dass die MDM-Aktivierung abgeschlossen ist.
19. Der BlackBerry UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
20. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet Konfigurationsinformationen an das Gerät.
21. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsupdates empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines macOS-Geräts



1. Stellen Sie sicher, dass der Benutzer ein BlackBerry UEM-Benutzerkonto und die folgenden Anmeldeinformationen für BlackBerry UEM Self-Service hat:
   - 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 auf Port 443.
4. BlackBerry UEM stellt das MDM-Profil für das Gerät bereit. In diesem Profil sind die MDM-Aktivierungs-URL und die Challenge enthalten. Das MDM-Profil ist als signierte PKCS#7-Nachricht gewrappt, in der die vollständige Zertifikatskette des Signaturgebers enthalten ist, wodurch es dem Gerät möglich ist, das Profil zu überprüfen. Dadurch wird der Anmeldungsvorgang ausgelöst.
5. Der native MDM-Daemon auf dem Gerät sendet das Geräteprofil, einschließlich der Kunden-ID, der Sprache und der Version des Betriebssystems, an BlackBerry UEM.
6. BlackBerry UEM überprüft, dass die Anforderung von einer Zertifizierungsstelle signiert wurde und auf den nativen MDM-Daemon mit einer erfolgreichen Authentifizierungsbenachrichtigung reagiert.
7. Der native MDM-Daemon sendet eine Anforderung an BlackBerry UEM, um ein Zertifizierungsstellenzertifikat, Funktionsinformationen der Zertifizierungsstelle und ein vom Gerät ausgegebenes Zertifikat anzufragen.
8. BlackBerry UEM sendet das Zertifizierungsstellenzertifikat, Funktionsinformationen der Zertifizierungsstelle und das vom Gerät ausgegebene Zertifikat an den nativen MDM-Daemon.
9. Der native MDM-Daemon installiert das MDM-Profil auf dem Gerät.
10. BlackBerry UEM bestätigt, dass die MDM-Aktivierung abgeschlossen ist.
11. Das Gerät fordert alle Konfigurationsinformationen an.
12. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet Konfigurationsinformationen an das Gerät.
13. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines Windows 10-Geräts

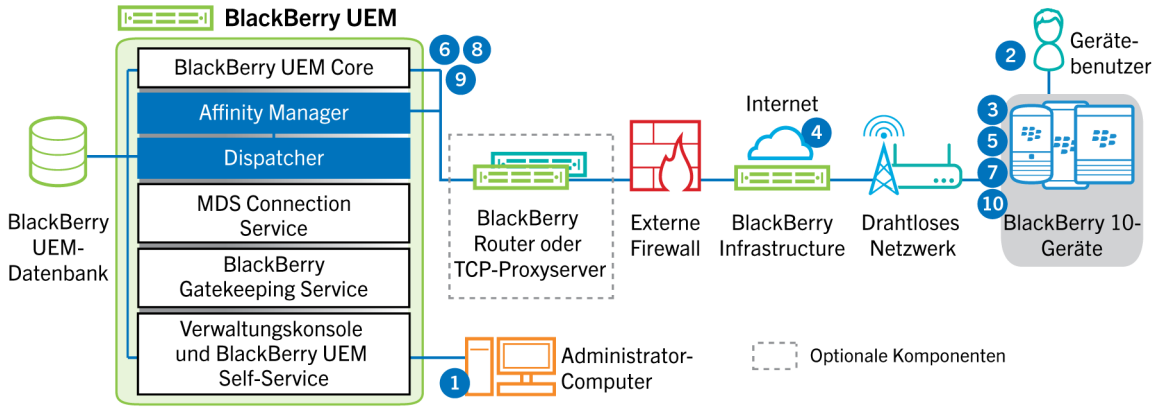


1. Führen Sie die folgenden Schritte aus:
   a. Konfigurieren Sie den Suchdienst, um die Windows 10-Aktivierungen zu vereinfachen.
   b. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
   c. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
      - Generieren Sie automatisch ein Geräteaktivierungskennwort, und senden Sie automatisch eine E-Mail mit Aktivierungsanweisungen für den Benutzer.
      - Richten Sie ein Geräteaktivierungskennwort ein, und wählen Sie die Option zum Senden der Aktivierungsinformationen per E-Mail an den Benutzer.
      - Richten Sie kein Geräteaktivierungskennwort ein, und senden Sie dem Benutzer eine Mitteilung an die BlackBerry UEM Self-Service-Adresse, sodass dieser ein eigenes Aktivierungskennwort festlegen kann.
   d. Stellen Sie dem Benutzer ein Zertifizierungsstellenzertifikat bereit, das von BlackBerry UEM generiert wurde und auf seinem Gerät installiert werden soll.
2. Der Benutzer führt folgende Aktionen auf seinem Gerät aus:
   a. Überprüfen, ob das Gerät über eine Internetverbindung auf Port 443 verfügt.
   b. Öffnen und Installieren des Zertifikats.
   c. Navigieren zu Einstellungen > Konten > Geschäftlicher Zugriff und Tippen auf Verbinden
   d. Wenn er dazu aufgefordert wird, gibt er seine E-Mail-Adresse und sein Aktivierungskennwort ein, das er mit der Aktivierungs-E-Mail erhalten hat.
3. Das Gerät stellt eine Verbindung zum Suchdienst her, den Sie konfiguriert haben, um Windows 10-Aktivierungen in Ihrem Unternehmen zu vereinfachen.
4. Der Suchdienst prüft, ob die SRP-ID für den BlackBerry UEM-Server gültig ist und leitet das Gerät an BlackBerry UEM weiter.
5. Das Gerät sendet eine Aktivierungsanforderung an BlackBerry UEM auf Port 443. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Gerätekennung.
6. BlackBerry UEM führt folgende Aktionen aus:
   a. Überprüfen der Anmeldeinformationen auf Gültigkeit
   b. Erstellen eines Gerätekennworts
   c. Verknüpfen der Geräteinstanz mit dem angegebenen Benutzerkonto in der BlackBerry UEM-Datenbank
   d. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
   e. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät
7. Das Gerät erstellt eine CSR und sendet sie über HTTPS an BlackBerry UEM. Die CSR enthält den Benutzernamen und das Aktivierungskennwort.

8. BlackBerry UEM überprüft den Benutzernamen und das Kennwort, überprüft die CSR und gibt das Client-Zertifikat und das Zertifizierungsstellenzertifikat an das Gerät zurück.

   Die gesamte Kommunikation zwischen dem Gerät und BlackBerry UEM basiert nun mithilfe dieser Zertifikate auf gegenseitiger und vollständiger Authentifizierung.
9. Das Gerät fordert alle Konfigurationsinformationen an.
10. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet Konfigurationsinformationen an das Gerät.
11. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Datenfluss: Aktivieren eines BlackBerry 10-Geräts



1. Führen Sie die folgenden Schritte aus:
   a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
   b. Weisen Sie dem Benutzer ein Aktivierungsprofil zu.
   c. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
      - Automatisches Generieren eines Geräteaktivierungskennworts und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer
      - Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzername und Kennwort 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 kann
2. Der Benutzer führt die folgenden Aktionen aus:
   a. Eingeben des Benutzernamens und des Aktivierungskennworts auf dem Gerät
   b. Im Fall einer Aktivierung vom Typ „Geschäftlich und persönlich – Reguliert“ oder „Nur geschäftlicher Bereich“ akzeptiert er die Geschäftsbedingungen des Unternehmens, denen der Benutzer zustimmen muss
3. Wenn es sich um eine Aktivierung vom Typ „Nur geschäftlicher Bereich“ handelt, werden auf dem Gerät alle bestehenden Daten gelöscht, und das Gerät wird neu gestartet. Für andere Aktivierungsarten führt der Enterprise Management Agent auf dem Gerät die folgenden Aktionen durch:
   a. Aufbau einer Verbindung mit der BlackBerry Infrastructure
   b. Sendet eine Anforderung bezüglich Aktivierungsinformationen an die BlackBerry Infrastructure
4. Die BlackBerry Infrastructure führt die folgenden Aktionen aus:
   a. Bestätigt, dass der Benutzer ein gültiger und registrierter Benutzer ist
   b. Ruft die BlackBerry UEM-Adresse für den Benutzer ab
   c. Sendet die Adresse an den Enterprise Management Agent
5. Das Gerät führt die folgenden Aktionen aus:
   a. Stellt eine Verbindung mit BlackBerry UEM her.
   b. Generiert einen gemeinsam genutzten symmetrischen Schlüssel, um die CSR zu schützen und BlackBerry UEM mittels des Aktivierungskennworts und EC-SPEKE zu antworten.
   c. Erstellt wie folgt eine verschlüsselte CSR und einen HMAC:
      - Generiert ein Schlüsselpaar für das Zertifikat
      - Erstellt eine PKCS#10 CSR, die den öffentlichen Schlüssel des Schlüsselpaars umfasst

- Verschlüsselt die CSR mithilfe des gemeinsamen symmetrischen Schlüssels und AES-256 im CBC-Modus mit PKCS#5-Padding
- Berechnet den HMAC der verschlüsselten CSR mithilfe von SHA-256 und hängt ihn an die CSR an

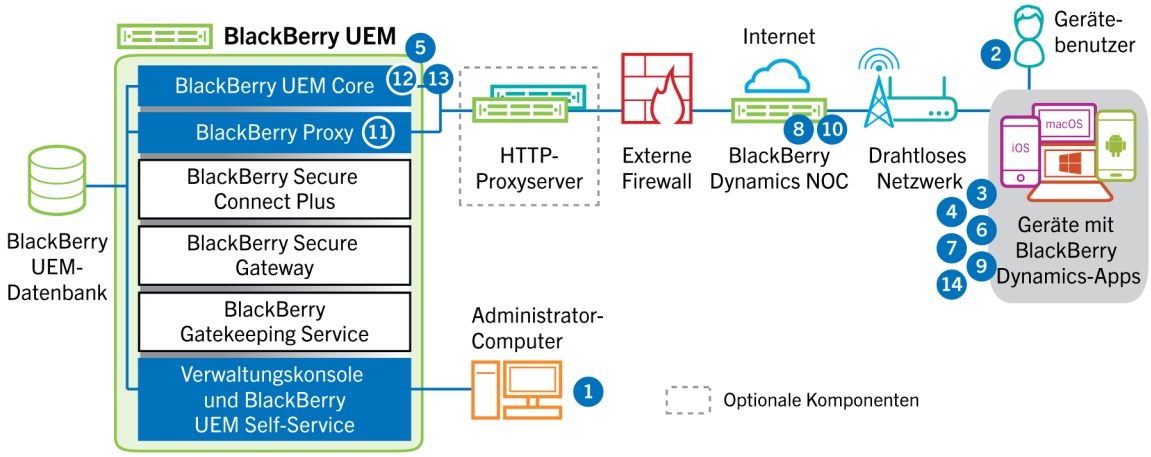
d. Sendet die verschlüsselte CSR und den HMAC an den BlackBerry UEM

6. BlackBerry UEM führt die folgenden Aktionen aus:
   a. Verifiziert den HMAC der verschlüsselten CSR und entschlüsselt die CSR mithilfe des gemeinsamen symmetrischen Schlüssels
   b. Ruft den Benutzernamen, die ID des geschäftlichen Bereichs sowie den Namen Ihres Unternehmens aus der BlackBerry UEM-Datenbank ab
   c. Verpackt das Client-Zertifikat mit den empfangenen Informationen und der vom Gerät gesendeten CSR
   d. Signiert das Client-Zertifikat mit dem Verwaltungsstammzertifikat des Unternehmens
   e. Verschlüsselt das Client-Zertifikat, das Verwaltungsstammzertifikat des Unternehmens und die BlackBerry UEM-URL mithilfe des gemeinsamen symmetrischen Schlüssels und AES-256 im CBC-Modus mit PKCS#5-Padding
   f. Berechnet einen HMAC des verschlüsselten Client-Zertifikats, des Verwaltungsstammzertifikats des Unternehmens und der BlackBerry UEM-URL und hängt ihn an die verschlüsselten Daten an
   g. Sendet die verschlüsselten Daten und den HMAC an das Gerät
7. Das Gerät führt die folgenden Aktionen aus:
   a. Verifiziert den HMAC
   b. Entschlüsselt die von BlackBerry UEM empfangenen Daten
   c. Speichert das Client-Zertifikat und das Verwaltungsstammzertifikat des Unternehmens in seinem Schlüsselspeicher
8. BlackBerry UEM führt die folgenden Aktionen aus:
   a. BlackBerry UEM Core weist das neue Gerät einer BlackBerry UEM-Instanz in der Domäne zu
   b. BlackBerry UEM Core teilt dem aktiven BlackBerry Affinity Manager mit, dass der BlackBerry UEM-Instanz ein neues Gerät zugewiesen wurde.
   c. Der aktive BlackBerry Affinity Manager benachrichtigt den BlackBerry Dispatcher auf dieser BlackBerry UEM-Instanz, dass ein neues Gerät vorliegt
   d. Der BlackBerry UEM Core sendet Konfigurationsinformationen, einschließlich Enterprise-Konnektivitätseinstellungen auf das Gerät.
9. BlackBerry UEM Core und das Gerät generieren den Transportschlüssel des Geräts mithilfe von ECMQV und der authentifizierten langfristig geltenden öffentlichen Schlüssel aus dem Client-Zertifikat und dem Server-Zertifikat für BlackBerry UEM. Der Schlüssel wird zum Verschlüsseln von geschäftlichen Daten verwendet, wenn BlackBerry Secure Connect Plus und Push oder IPPP nicht für die Datenübertragung verwendet werden.
10. Das Gerät sendet eine Bestätigung über TLS an BlackBerry UEM, die angibt, dass es die IT-Richtlinie und die anderen Daten empfangen und angewendet hat und dass es den geschäftlichen Bereich erstellt hat. Der Aktivierungsprozess ist abgeschlossen.

Die im Aktivierungsprozess herangezogenen Protokolle auf Basis elliptischer Kurven verwenden die von NIST empfohlene 521-Bit-Kurve.

Datenfluss: Aktivieren einer BlackBerry Dynamics-App

Dieser Datenfluss beschreibt, wie die Daten übertragen werden, wenn eine BlackBerry Dynamics-App aktiviert wird.



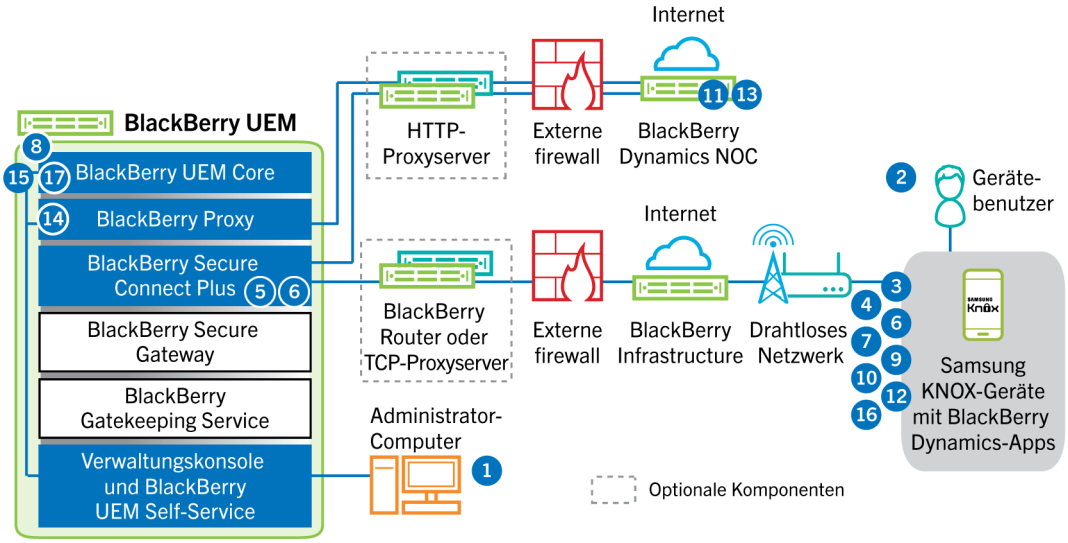
1. Ein Administrator weist einem Benutzer BlackBerry Dynamics-Apps zu.
2. Der Benutzer installiert die App auf seinem Gerät.
3. Wenn das Gerät kein Samsung Knox Workspace-Gerät ist und der BlackBerry UEM Client auf dem Gerät installiert ist, führt die BlackBerry Dynamics-App die folgenden Aktionen durch:
   a. Sie stellt einen sicheren Kanal mit dem BlackBerry UEM Client auf dem Gerät her. Die über den sicheren Kanal ausgetauschten Daten werden mit einem AES-CBC-Chiffrierschlüssel verschlüsselt.
   b. Sie fordert den BlackBerry UEM Client auf, einen Zugriffsschlüssel für die neue BlackBerry Dynamics-App anzufordern. Diese Anforderung bezieht sich auf eine zufällig generierte Zeichenfolge (Nonce).
4. Eines der folgenden Ereignisse tritt auf:
   - Der BlackBerry UEM Client sendet die Zugriffsschlüsselanfrage und die zufällig generierte Zeichenfolge an den BlackBerry UEM Core.
   - Wenn der BlackBerry UEM Client nicht auf dem Gerät installiert ist oder das Gerät Samsung Knox Workspace verwendet und dies die erste aktivierte BlackBerry Dynamics-App ist, erzeugt der Administrator einen Zugriffsschlüssel für den Benutzer oder der Benutzer meldet sich bei BlackBerry UEM Self-Service an und erzeugt einen Zugriffsschlüssel.
   - Wenn das Gerät oder Knox Workspace bereits eine aktivierte BlackBerry Dynamics-App enthält, sendet die aktivierte App eine Anfrage für einen Zugriffsschlüssel und die zufällig generierte Zeichenfolge an den BlackBerry UEM Core.
5. Der BlackBerry UEM Core sendet den angeforderten Zugriffsschlüssel an den BlackBerry UEM Client.
6. Der BlackBerry UEM Client stellt den Zugriffsschlüssel für die BlackBerry Dynamics-App bereit.
7. Die BlackBerry Dynamics-App stellt eine SSL-Verbindung mit dem BlackBerry Dynamics NOC her und sendet diesem einen Hash des Zugriffsschlüssels.
8. Das BlackBerry Dynamics NOC verifiziert den Zugriffsschlüssel und sendet nach erfolgreicher Verifizierung die Bereitstellungsdaten, einschließlich Masterschlüssel-Link und Verbindungsdaten, an die BlackBerry Dynamics-App.
9. Die BlackBerry Dynamics-App beginnt mit dem Einrichtungsprozess eines gemeinsamen geheimen Schlüssels mit dem BlackBerry UEM Core, indem sie eine Nachricht über den Aufbau eines sicheren Kanals an das BlackBerry Dynamics NOC über die SSL-Verbindung sendet.

Die Nachricht über die Einrichtung eines sicheren Kanals beinhaltet einen Benutzerbezeichner (E-Mail-Adresse), einen kurzlebigen öffentlichen ECDH-Schlüssel, einen Salt-Wert, ein Token und einen MAC der Nachricht für die Authentifizierung des Absenders und als Garantie der Nachrichtenintegrität.

10. Das BlackBerry Dynamics NOC leitet die Nachricht über die Einrichtung eines sicheren Kanals über eine HTTPS-Verbindung an den BlackBerry Proxy.
11. Der BlackBerry Proxy leitet diese Nachricht dann weiter an den BlackBerry UEM Core.
12. Der BlackBerry UEM Core sendet eine Antwort an die BlackBerry Dynamics-App. Die Antwort beinhaltet einen neuen kurzlebigen öffentlichen ECDH-Schlüssel einen MAC der Nachricht.
13. Die BlackBerry Dynamics-App fordert die Bereitstellungsdaten vom BlackBerry UEM Core an. Die Anforderung wird über das BlackBerry Dynamics NOC und den BlackBerry Proxy geleitet.
14. Der BlackBerry UEM Core sendet verschlüsselte Bereitstellungdaten, z. B. Master-Sitzungsschlüssel, App-Konfigurationsdaten und eine Liste der BlackBerry Proxy-Instanzen an die BlackBerry Dynamics-App, um die Aktivierung abzuschließen.

Datenfluss: Aktivieren einer BlackBerry Dynamics-App auf einem Samsung Knox Workspace-Gerät, wenn BlackBerry Secure Connect Plus aktiviert ist

Dieser Datenfluss beschreibt, wie die Daten übertragen werden, wenn eine BlackBerry Dynamics-App im geschäftlichen Bereich auf einem Samsung Knox Workspace-Gerät über eine BlackBerry Secure Connect Plus-Verbindung aktiviert wird.



1. Ein Administrator weist einem Benutzer BlackBerry Dynamics-Apps zu.
2. Der Benutzer installiert die App auf dem Samsung Knox-Gerät.
3. Wenn das Gerät kein Samsung Knox Workspace-Gerät ist und der BlackBerry UEM Client auf dem Gerät installiert ist, führt die BlackBerry Dynamics-App die folgenden Aktionen durch:
   a. Sie stellt einen sicheren Kanal mit dem BlackBerry UEM Client auf dem Gerät her. Die über den sicheren Kanal ausgetauschten Daten werden mit einem AES-CBC-Chiffrierschlüssel verschlüsselt.
   b. Sie fordert den BlackBerry UEM Client auf, einen Zugriffsschlüssel für die neue BlackBerry Dynamics-App anzufordern. Diese Anforderung bezieht sich auf eine zufällig generierte Zeichenfolge (Nonce).
4. Das Gerät sendet eine Anfrage über einen TLS-Tunnel und Port 443 an die BlackBerry Infrastructure, 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.
5. BlackBerry Secure Connect Plus empfängt die Anforderung von der BlackBerry Infrastructure über Port 3101.
6. 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.
7. Der BlackBerry UEM Client sendet die Zugriffsschlüsselanfrage und die zufällig generierte Zeichenfolge vom BlackBerry Secure Connect Plus an den BlackBerry UEM Core.
8. Der BlackBerry UEM Core sendet den angeforderten Zugriffsschlüssel vom BlackBerry Secure Connect Plus an den BlackBerry UEM Client.
9. Der BlackBerry UEM Client stellt den Zugriffsschlüssel für die BlackBerry Dynamics-App bereit.
10. Die BlackBerry Dynamics-App stellt mit BlackBerry Secure Connect Plus eine Verbindung mit dem BlackBerry Dynamics NOC her und sendet diesem einen Hash des Zugriffsschlüssels.

11. Das BlackBerry Dynamics NOC verifiziert den Zugriffsschlüssel und sendet nach erfolgreicher Verifizierung die Bereitstellungsdaten, einschließlich Masterschlüssel-Link und Verbindungsdaten, mit BlackBerry Secure Connect Plus an die BlackBerry Dynamics-App.
12. Die BlackBerry Dynamics-App beginnt mit dem Einrichtungsprozess eines gemeinsamen geheimen Schlüssels mit dem BlackBerry UEM Core, indem sie eine Nachricht über den Aufbau eines sicheren Kanals an das BlackBerry Dynamics NOC mit BlackBerry Secure Connect Plus sendet.

    Die Nachricht über die Einrichtung eines sicheren Kanals beinhaltet einen Benutzerbezeichner (E-Mail-Adresse), einen kurzlebigen öffentlichen ECDH-Schlüssel, einen Salt-Wert, ein Token und einen MAC der Nachricht für die Authentifizierung des Absenders und als Garantie der Nachrichtenintegrität.
13. Das BlackBerry Dynamics NOC leitet die Nachricht über die Einrichtung eines sicheren Kanals über eine HTTPS-Verbindung an den BlackBerry Proxy.
14. Der BlackBerry Proxy leitet diese Nachricht dann weiter an den BlackBerry UEM Core.
15. Der BlackBerry UEM Core sendet eine Antwort an die BlackBerry Dynamics-App mithilfe vom BlackBerry Secure Connect Plus. Die Antwort beinhaltet einen neuen kurzlebigen öffentlichen ECDH-Schlüssel einen MAC der Nachricht.
16. Die BlackBerry Dynamics-App fordert die Bereitstellungsdaten vom BlackBerry UEM Core an. Die Anforderung wird über BlackBerry Secure Connect Plus, das BlackBerry Dynamics NOC und den BlackBerry Proxy geleitet.
17. Der BlackBerry UEM Core sendet verschlüsselte Bereitstellungdaten, z. B. Master-Sitzungsschlüssel, App-Konfigurationsdaten und eine Liste der BlackBerry Proxy-Instanzen an die BlackBerry Dynamics-App, um die Aktivierung abzuschließen.

Senden und Empfangen von geschäftlichen Daten

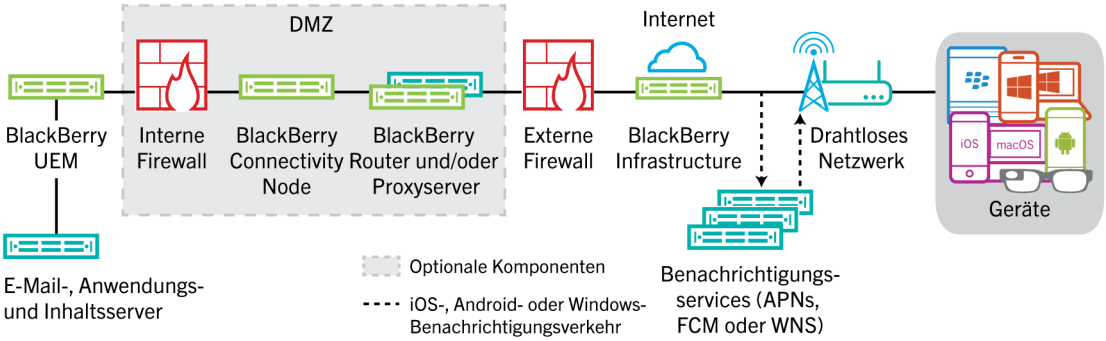
Wenn Geräte, die auf BlackBerry UEM aktiv sind, geschäftliche Daten senden und empfangen, stellen sie eine Verbindung mit den E-Mail-, Anwendungs- oder Inhaltsservern Ihres Unternehmens her. Zum Beispiel stellen Geräte eine Verbindung mit dem E-Mail-Server Ihres Unternehmens her, wenn sie die geschäftlichen E-Mail- oder Kalender-Apps verwenden. Wenn sie den geschäftlichen Browser verwenden, um im Intranet zu navigieren, stellen sie eine Verbindung mit dem Webserver in Ihrem Unternehmen her.

Je nach Typ des Geräts, der Aktivierungsart, den Lizenztypen und Konfigurationseinstellungen, kann ein Gerät Verbindungen zu den Servern Ihres Unternehmens über die folgenden Pfade herstellen:

Datenpfad	Beschreibung
Wi-Fi-Geschäftsnetzwerk	Sie können BlackBerry UEM zum Konfigurieren von Wi-Fi-Profilen für Geräte verwenden, damit Geräte auf die Ressourcen Ihres Unternehmens über Ihr geschäftliches Wi-Fi-Netzwerk zugreifen können.
VPN	Sie können BlackBerry UEM für die Konfiguration von VPN-Profilen für Geräte verwenden, oder Benutzer können VPN-Profile auf ihren Geräten konfigurieren, die den Zugriff auf Ressourcen Ihres Unternehmens über VPN zulassen.
BlackBerry UEM und die BlackBerry Infrastructure oder BlackBerry Dynamics NOC	Je nach Art des Geräts, der Aktivierung und der Lizenz und je nach vorhandenen BlackBerry Dynamics-Apps können Geräte möglicherweise Enterprise-Konnektivität für die Kommunikation Ihrer Unternehmensressourcen über BlackBerry UEM und die BlackBerry Infrastructure nutzen. • Bei iOS-Geräten mit der entsprechenden Lizenz können Sie den BlackBerry Secure Gateway aktivieren, um Geräten das Herstellen einer Verbindung zum geschäftlichen E-Mail-Server über die BlackBerry Infrastructure und BlackBerry UEM zu ermöglichen. Wenn Sie den BlackBerry Secure Gateway verwenden, müssen Sie Ihren E-Mail-Server nicht außerhalb der Firewall verfügbar machen, damit Benutzer mit iOS-Geräten eine Verbindung zu Microsoft Exchange herstellen können, wenn keine Verbindung zum VPN oder dem geschäftlichen Wi-Fi-Netzwerk besteht. • Für Geräte mit BlackBerry 10, iOS, Android Enterprise und Samsung Knox Workspace, die über eine entsprechende Lizenz verfügen, können Sie durch Aktivierung von BlackBerry Secure Connect Plus Enterprise-Konnektivität verwenden. Wenn diese Geräte BlackBerry Secure Connect Plus nutzen, werden die geschäftlichen Daten in einem sicheren IP-Tunnel zwischen den Apps auf dem Gerät und dem Netzwerk Ihres Unternehmens über die BlackBerry Infrastructure übertragen. • Die auf Geräten installierten BlackBerry Dynamics-Apps kommunizieren mit dem BlackBerry Proxy. Je nach Konfiguration können Daten über BlackBerry Dynamics NOC oder die BlackBerry Infrastructure geleitet werden oder mithilfe von BlackBerry Dynamics Direct Connect beide umgehen. • BlackBerry 10-Geräte können Enterprise-Konnektivität für alle geschäftlichen Daten verwenden. Enterprise-Konnektivität verschlüsselt und authentifiziert alle geschäftlichen Daten und sendet sie über BlackBerry UEM und die BlackBerry Infrastructure. Die Enterprise-Konnektivität schränkt die Anzahl der Ports, die Sie in der externen Firewall Ihres Unternehmens öffnen müssen, auf einen Port ein: 3101.

Senden und Empfangen von geschäftlichen Daten mit der BlackBerry Infrastructure

Geräte stellen eine Verbindung zu BlackBerry UEM über die BlackBerry Infrastructure her, um Konfigurations-Updates zu erhalten und geschäftliche Daten mittels Enterprise-Konnektivität oder BlackBerry Secure Gateway zu senden und zu empfangen. Das folgende Diagramm zeigt, wie Geräte eine Verbindung zu BlackBerry UEM und den Ressourcen Ihrer Organisation über die BlackBerry Infrastructure herstellen.



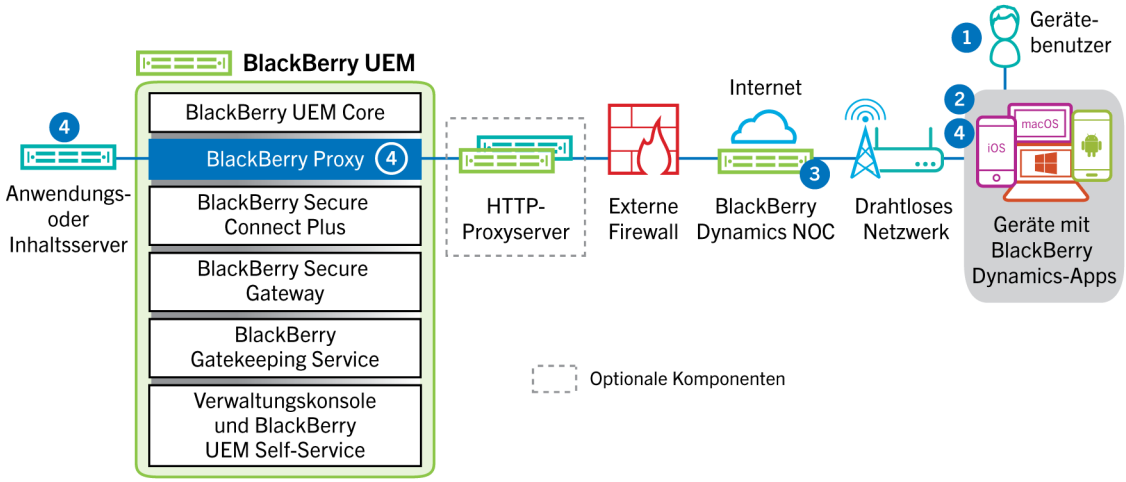
In der folgenden Tabelle werden die Situationen aufgeführt, in denen Geräte eine Verbindung zu BlackBerry UEM und zum Netzwerk Ihres Unternehmens über die BlackBerry Infrastructure herstellen.

Gerätetyp	Beschreibung
Alle Geräte	Alle Geräte verwenden diesen Kommunikationspfad zum Senden und Empfangen von Konfigurationsdaten, wie Gerätebefehle, Richtlinien- und Profil-Updates, und zum Senden von Geräteinformationen und Aktivitätsberichten. Weitere Informationen finden Sie unter Empfangen von Konfigurationsupdates für Geräte.
iOS-Geräte	Sie können BlackBerry Secure Gateway aktivieren, um iOS-Geräten das Herstellen einer Verbindung zu Ihrem geschäftlichen E-Mail-Server über die BlackBerry Infrastructure und BlackBerry UEM zu ermöglichen. Wenn Sie den BlackBerry Secure Gateway verwenden, müssen Sie Ihren E-Mail-Server nicht außerhalb der Firewall verfügbar machen, damit Benutzer geschäftliche E-Mails empfangen können, wenn keine Verbindung zum VPN Ihres Unternehmens oder dem geschäftlichen Wi-Fi-Netzwerk besteht.

Gerätetyp	Beschreibung
iOS-, Android Enterprise-, Samsung Knox Workspace und BlackBerry 10-Geräte.	Geräte, die über ein Enterprise-Konnektivitätsprofil verfügen, das für die Verwendung von BlackBerry Secure Connect Plus konfiguriert ist, können einen sicheren IP-Tunnel über die BlackBerry Infrastructure zum Übertragen von Daten zwischen Apps und dem Netzwerk Ihres Unternehmens verwenden. Für iOS-Geräte kann BlackBerry Secure Connect Plus einen sicheren Tunnel zwischen Ihrem Unternehmensnetzwerk und allen Apps oder nur den angegebenen Apps bereitstellen. Für Android Enterprise- und BlackBerry 10-Geräte bietet BlackBerry Secure Connect Plus einen sicheren Tunnel zwischen Apps für den geschäftlichen Bereich und dem Netzwerk Ihres Unternehmens. 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.
iOS- und Android-Geräte, auf denen BlackBerry Dynamics-Apps installiert sind	Wenn Enterprise-Konnektivität für BlackBerry Dynamics-Apps verwendet wird, ist die BlackBerry Infrastructure nicht erforderlich. Stattdessen werden Daten, die zwischen BlackBerry Dynamics-Apps und BlackBerry Proxy übertragen werden, über das BlackBerry Dynamics NOC geleitet oder umgehen das NOC bei Verwendung von BlackBerry Dynamics Direct Connect.
BlackBerry 10-Geräte	BlackBerry 10-Geräte nutzen diesen Kommunikationspfad zum Senden und Empfangen von geschäftlichen Daten, wenn es sich dabei um die direkteste, kosteneffektivste Route handelt, die verfügbar ist.

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

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



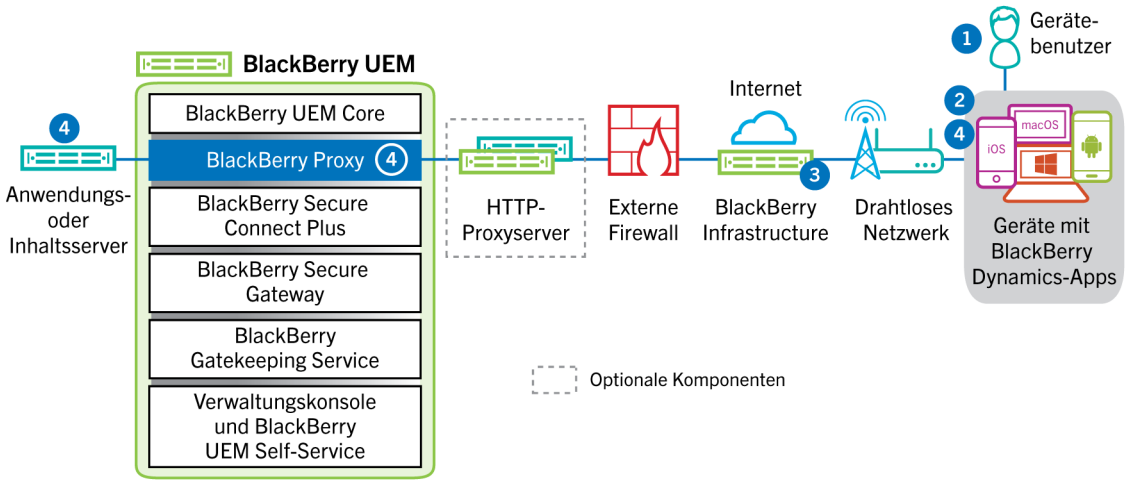
1. Der Benutzer öffnet eine BlackBerry Dynamics-App, um auf geschäftliche Daten zuzugreifen.

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 kommuniziert mit dem BlackBerry Proxy über eine zuvor erstellte sichere Verbindung, die den Aufbau einer durchgehenden Verbindung für geschäftliche Daten zwischen der BlackBerry Dynamics-App und dem BlackBerry Proxy ermöglicht. Die geschäftlichen Daten werden mit einem Sitzungsschlüssel verschlüsselt, der dem BlackBerry Dynamics NOC nicht 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.

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

Je nach Serverkonfiguration können geschäftliche Daten für Apps, die mit BlackBerry Dynamics SDK 7.0 und höher entwickelt wurden, über die BlackBerry Infrastructure statt über BlackBerry Dynamics NOC geleitet werden. Wenn Sie über eine neue Installation von BlackBerry UEM Version 12.12 verfügen, verwendet BlackBerry UEM standardmäßig die BlackBerry Infrastructure. Wenn Sie ein Upgrade von einer früheren BlackBerry UEM Version durchgeführt haben, müssen Sie sich zum Aktivieren dieser Funktion an den technischen Support von BlackBerry wenden.

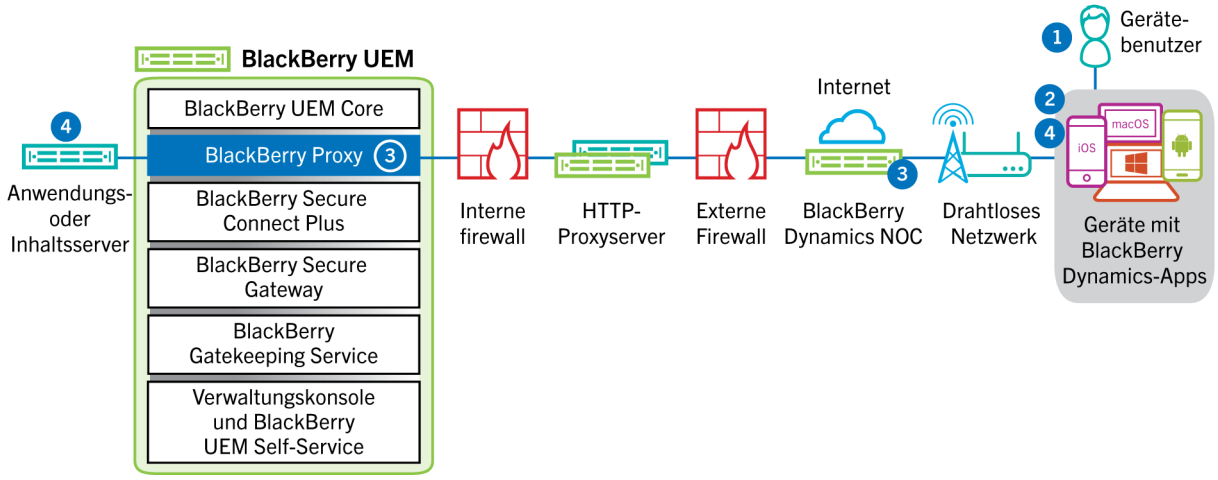
Dieser Datenfluss beschreibt, wie Daten übertragen werden, wenn eine BlackBerry Dynamics-App auf einen Anwendungs- oder einen Inhaltsserver in Ihrem Unternehmen über BlackBerry Infrastructure und BlackBerry UEM zugreift.



1. Der Benutzer öffnet eine BlackBerry Dynamics-App, um auf geschäftliche Daten zuzugreifen.
2. Die BlackBerry Dynamics-App baut eine Verbindung mit dem BlackBerry Infrastructure auf.
3. Die BlackBerry Infrastructure kommuniziert mit BlackBerry Proxy über eine vorab eingerichtete TLS-Verbindung.
4. Die BlackBerry Dynamics-App stellt eine TLS-Verbindung zum BlackBerry Proxy her, und geschäftliche Daten werden über eine sichere End-to-End-Verbindung ausgetauscht.

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 UEM zugreift. Weitere Informationen zu Direct Connect finden Sie unter Konfigurieren von Direct Connect mit BlackBerry UEM.

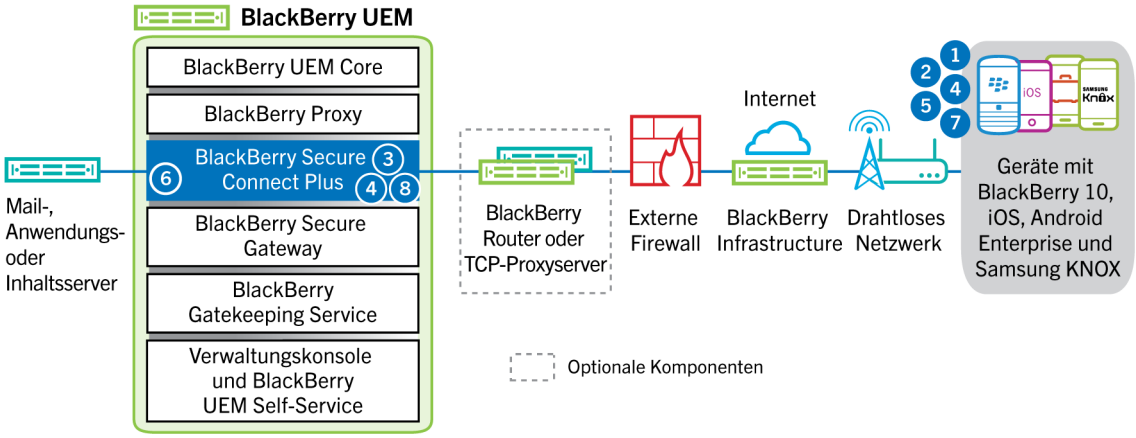


1. Der Benutzer öffnet eine BlackBerry Dynamics-App, um auf geschäftliche Daten zuzugreifen.
2. Die BlackBerry Dynamics-App baut eine TLS-Verbindung mit BlackBerry Proxy auf.
3. BlackBerry Proxy authentifiziert sich bei der BlackBerry Dynamics-App. BlackBerry Proxy authentifiziert sich mit seinem Serverzertifikat 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.

Datenfluss: Zugreifen auf einen Anwendungs- oder Inhaltsserver mithilfe von 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.

Dieser Datenfluss gilt nicht für BlackBerry Dynamics-Apps im geschäftlichen Bereich auf Android Enterprise- oder Samsung Knox Workspace-Geräten. Weitere Informationen finden Sie unter Datenfluss: Senden und Empfangen von geschäftlichen Daten von einer BlackBerry Dynamics-App auf einem Android-Gerät unter Verwendung von BlackBerry Secure Connect Plus



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-Geräten verwenden alle Apps für den geschäftlichen Bereich BlackBerry Secure Connect Plus, außer die Apps, die Sie einschränken.
- Für Samsung Knox Workspace-Geräte geben Sie an, ob alle oder nur die angegebenen Apps des geschäftlichen Bereichs BlackBerry Secure Connect Plus verwenden.
- Für iOS-Geräte geben Sie an, ob alle oder nur die angegebenen Apps BlackBerry Secure Connect Plus verwenden.
- Auf BlackBerry 10- und Android Enterprise-Geräten verwenden alle Apps des geschäftlichen Bereichs BlackBerry Secure Connect Plus.

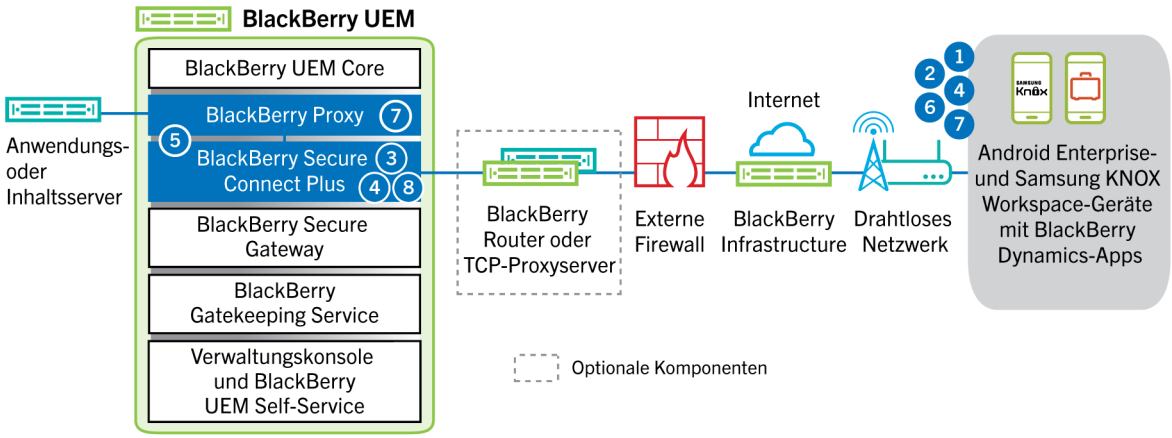
2. Das Gerät sendet eine Anfrage über einen TLS-Tunnel und Port 443 an die BlackBerry Infrastructure, um einen sicheren Tunnel zum Netzwerk des Unternehmens anzufordern. Das Signal wird standardmäßig mit FIPS-140-zertifizierten Certicom-Bibliotheken verschlüsselt. Der Tunnel für das Signal ist komplett verschlüsselt.
3. BlackBerry Secure Connect Plus empfängt die Anforderung von der BlackBerry 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.

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.

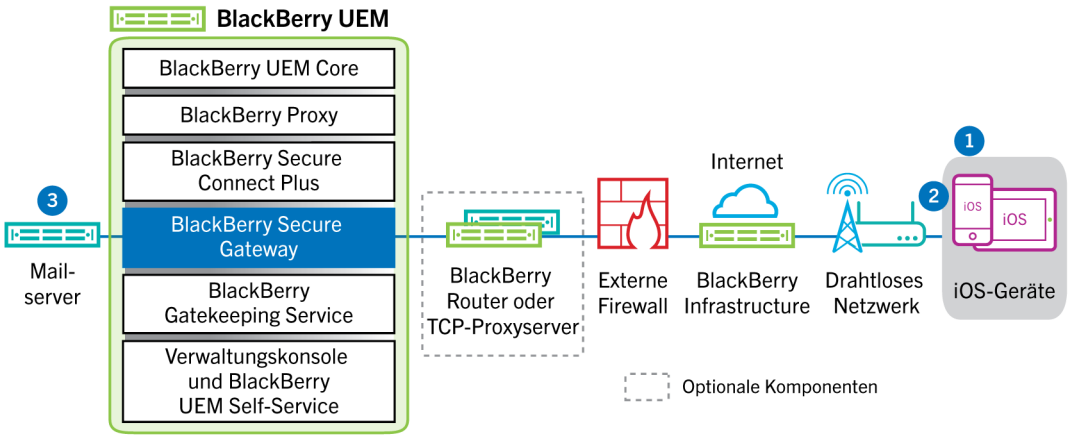
Wenn Sie BlackBerry Secure Connect Plus mit BlackBerry Dynamics-Apps auf einem Android Enterprise-Gerät oder ein Samsung Knox Workspace-Gerät verwenden, wird empfohlen, dass Sie BlackBerry UEM konfigurieren, damit sie keine BlackBerry Dynamics-App-Daten über BlackBerry Dynamics NOC sendet, um Netzwerklatenz 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 Infrastructure, 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 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. 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 einer E-Mail von einem iOS-Gerät mithilfe des BlackBerry Secure Gateway

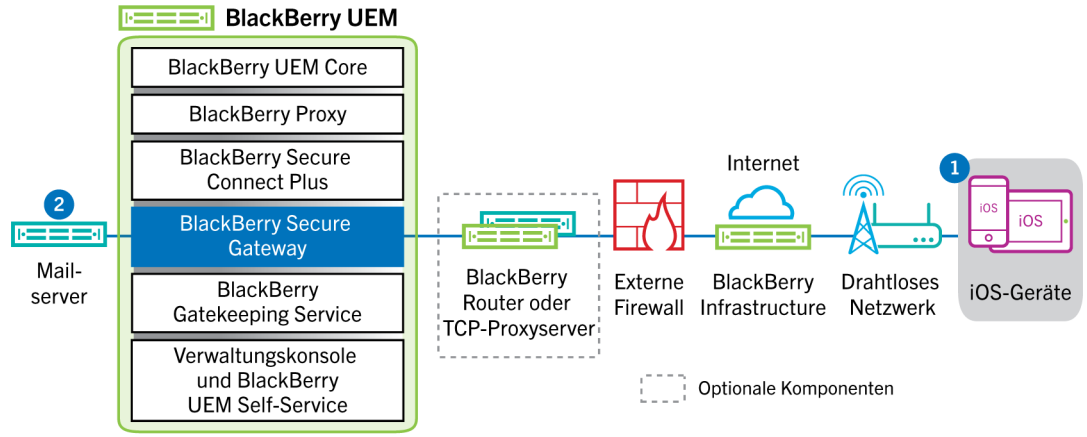
Dieser Datenfluss beschreibt, wie geschäftliche E-Mail- und Kalenderdaten von iOS-Geräten mithilfe des BlackBerry Secure Gateway zum Exchange ActiveSync-Server übertragen werden.



1. Ein Benutzer erstellt eine E-Mail oder aktualisiert ein Terminplanerelement 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 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 iOS-Gerät mithilfe von BlackBerry Secure Gateway

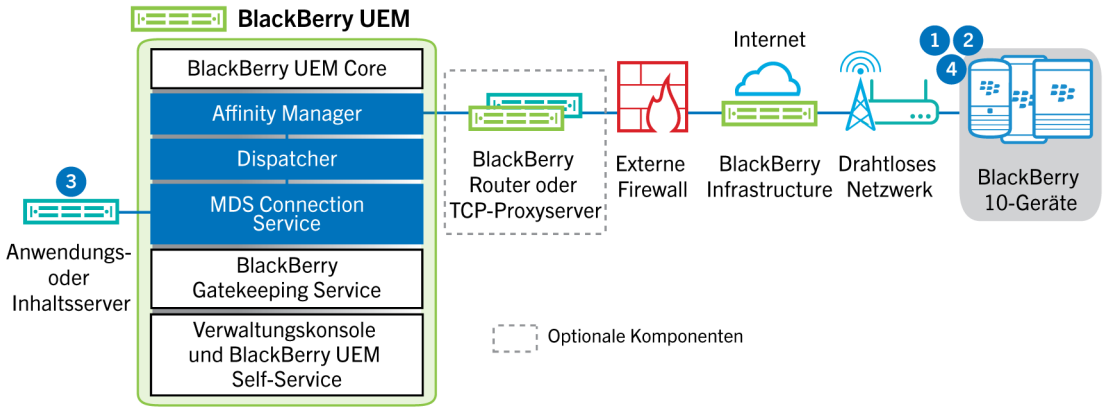
Dieser Datenfluss beschreibt, wie geschäftliche E-Mail- und Kalenderdaten zwischen iOS-Geräten und dem Exchange ActiveSync-Server mithilfe des BlackBerry Secure Gateway übertragen werden.



1. Der native E-Mail-Client auf dem iOS-Gerät stellt eine permanente Verbindung mit dem E-Mail-Server über einen verschlüsselten und authentifizierten Kanal zwischen der BlackBerry Infrastructure und BlackBerry Secure Gateway bereit und erkennt Änderungen in den für die Synchronisierung auf dem Mailserver konfigurierten Ordnern.
2. Sind für das Gerät neue oder geänderte Elemente vorhanden, wie eine neue E-Mail-Nachricht oder ein aktualisierter Kalendereintrag, sendet der E-Mail-Server die Updates über den sicheren Kanal, der zwischen BlackBerry Secure Gateway und der BlackBerry Infrastructure erstellt wurde, über das Exchange ActiveSync-Protokoll an die E-Mail- oder Terminplaner-App auf dem Gerät.

Datenfluss: Zugreifen auf einen Anwendungs- oder Inhaltsserver von einem BlackBerry 10-Gerät

Dieser Datenfluss beschreibt, wie Daten übertragen werden, wenn eine geschäftliche App auf einem BlackBerry 10-Gerät auf eine Anwendung oder einen Inhaltsserver zugreift und BlackBerry Secure Connect Plus deaktiviert ist.



1. Der Benutzer öffnet eine geschäftliche App, um geschäftliche Daten anzuzeigen. Zum Beispiel öffnet der Benutzer den geschäftlichen Browser, um im Intranet zu navigieren oder er verwendet BlackBerry Work Drives, um auf eine Datei auf einem Netzlaufwerk zuzugreifen.
2. Die App stellt eine Verbindung mit dem Anwendungs- oder Inhaltsserver her, um die Daten abzurufen. Die Anforderung wird über die BlackBerry Infrastructure, den BlackBerry Affinity Manager, den BlackBerry Dispatcher und den BlackBerry MDS Connection Service zum Anwendungs- oder Inhaltsserver geleitet.
3. Der Anwendungs- oder Inhaltsserver antwortet mit den geschäftlichen Daten. Die geschäftlichen Daten werden über den BlackBerry MDS Connection Service, den BlackBerry Dispatcher, BlackBerry Affinity Manager und die BlackBerry Infrastructure zum Gerät geleitet.
4. Die App empfängt die Daten und zeigt sie auf dem Gerät an.

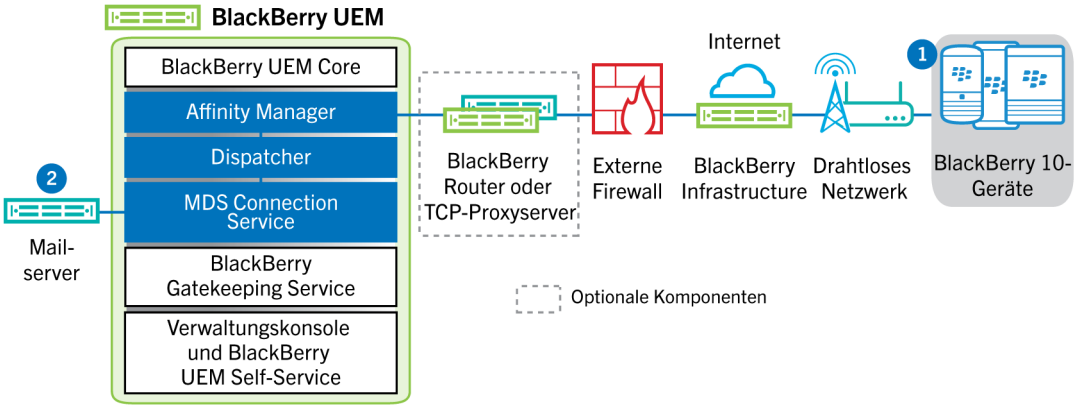
Datenfluss: Senden einer E-Mail von einem BlackBerry 10-Gerät

Dieser Datenfluss beschreibt, wie geschäftliche E-Mail- und Kalenderdaten von BlackBerry 10-Geräten zum Exchange ActiveSync-Server übertragen werden, wenn BlackBerry Secure Connect Plus nicht aktiviert ist.

1. Ein Benutzer erstellt eine E-Mail oder aktualisiert ein Terminplanerelement im geschäftlichen Bereich.
2. Das neue oder geänderte Element wird vom Gerät über die BlackBerry Infrastructure, BlackBerry Affinity Manager, BlackBerry Dispatcher und den BlackBerry MDS Connection Service an den E-Mail-Server gesendet.
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 von E-Mail auf BlackBerry 10-Geräten

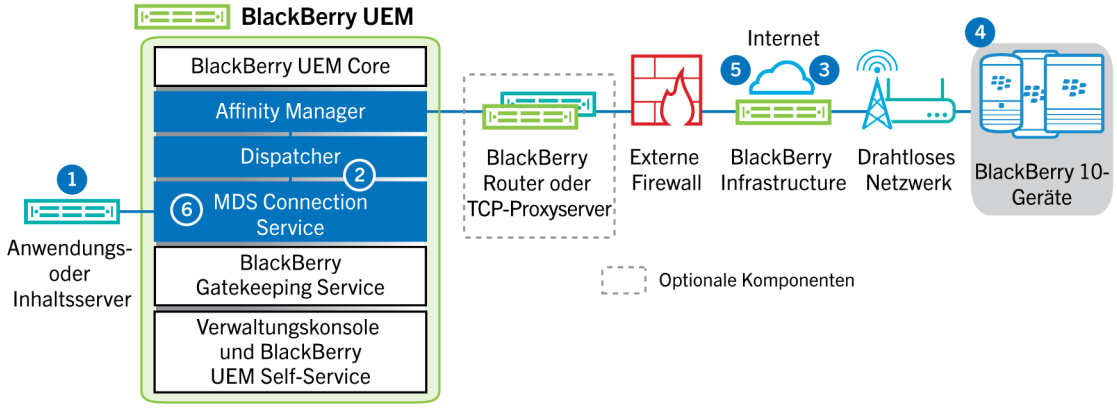
Dieser Datenfluss beschreibt den Empfang geschäftlicher E-Mail-Nachrichten vom Exchange ActiveSync-Server auf BlackBerry 10-Geräten, wenn BlackBerry Secure Connect Plus nicht aktiviert ist.



1. Der native E-Mail-Client auf dem Gerät stellt eine permanente Verbindung mit dem E-Mail-Server auf einem verschlüsselten und authentifizierten Kanal über die BlackBerry Infrastructure, BlackBerry Affinity Manager, BlackBerry Dispatcher und BlackBerry MDS Connection Service bereit und erkennt Änderungen in den für die Synchronisierung auf dem Mailserver konfigurierten Ordnern.
2. Sind für das Gerät neue oder geänderte Elemente vorhanden, wie eine neue E-Mail-Nachricht oder ein aktualisierter Kalendereintrag, sendet der E-Mail-Server die Updates unter Verwendung des Exchange ActiveSync-Protokolls über den BlackBerry MDS Connection Service, BlackBerry Dispatcher, BlackBerry Affinity Manager und die BlackBerry Infrastructure an die E-Mail- oder Terminplaner-App auf dem Gerät.

Datenfluss: Empfangen von Unternehmens-Push-Updates auf einem BlackBerry 10-Gerät

Dieser Datenfluss beschreibt, wie geschäftliche Daten zwischen einem Anwendungsserver und einer entsprechenden App in einem geschäftlichen Bereich eines BlackBerry 10-Geräts übertragen werden, wenn BlackBerry Secure Connect Plus deaktiviert ist.

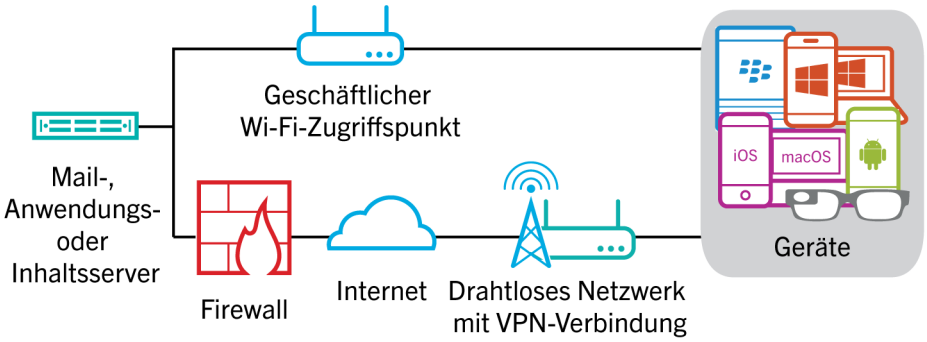


1. Wenn für eine geschäftliche App auf einem BlackBerry 10-Gerät neue oder aktualisierte Daten vorhanden sind, überträgt der Anwendungs- oder der Inhaltsserver die Daten an den BlackBerry MDS Connection Service mithilfe einer HTTP- oder HTTPS-Anforderung.
2. Der BlackBerry MDS Connection Service sendet die mit Push übertragenen Daten über den BlackBerry Dispatcher, BlackBerry Affinity Manager und die BlackBerry Infrastructure über Port 3101 in der Firewall.
3. Die BlackBerry Infrastructure sendet die Daten an das BlackBerry 10-Gerät.
4. Das BlackBerry 10-Gerät sendet eine Empfangsbestätigung an die BlackBerry Infrastructure. Die Geräte-App erkennt den eingehenden Inhalt und zeigt diesen an, wenn der Benutzer die App öffnet.
5. Die BlackBerry Infrastructure sendet eine Empfangsbestätigung über den BlackBerry Affinity Manager und den BlackBerry Dispatcher an den BlackBerry MDS Connection Service.
6. Bei entsprechender Konfiguration sendet der BlackBerry MDS Connection Service die Empfangsbestätigung mithilfe einer HTTP-Anforderung an den Push-Auslöser.

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.



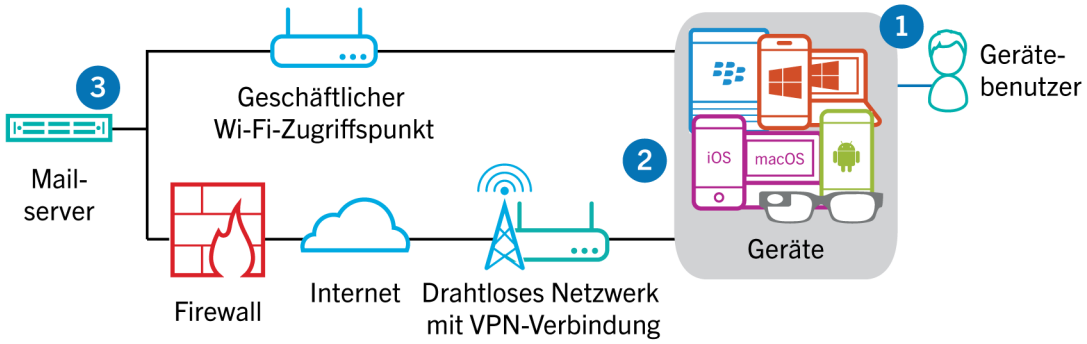
In der folgenden Tabelle wird beschrieben, wann Geräte über das VPN oder das geschäftliche Wi-Fi-Netzwerk Ihres Unternehmens eine Verbindung mit dem Unternehmensnetzwerk herstellen.

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.

Gerätetyp	Beschreibung
BlackBerry 10	BlackBerry 10-Geräte nutzen das VPN Ihres Unternehmens oder das geschäftliche Wi-Fi-Netzwerk zum Senden und Empfangen von geschäftlichen Daten, wenn es sich dabei um die direkteste, kosteneffektivste Route handelt, die verfügbar ist. BlackBerry 10-Geräte verwenden beim Zugriff auf geschäftliche Daten nur VPN- und Wi-Fi-Profile, die Sie konfiguriert haben, nicht ein Benutzer.

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

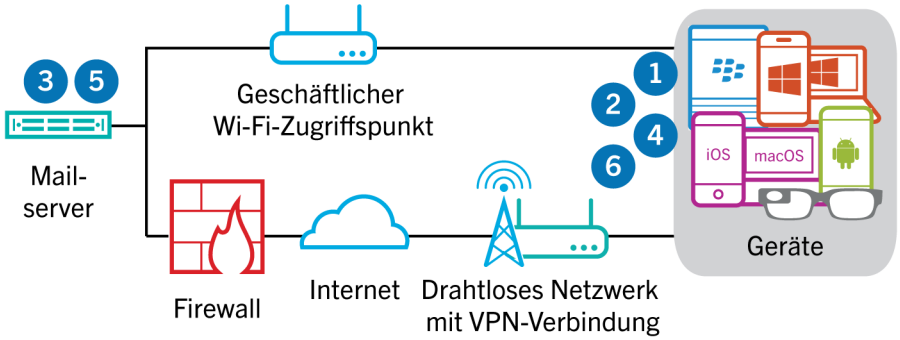
Dieser Datenfluss beschreibt, wie E-Mail- und Kalenderdaten von dem Gerät zum E-Mail-Server über das VPN Ihres Unternehmens oder das geschäftliche Wi-Fi-Netzwerk mithilfe von Exchange ActiveSync übertragen werden.



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.

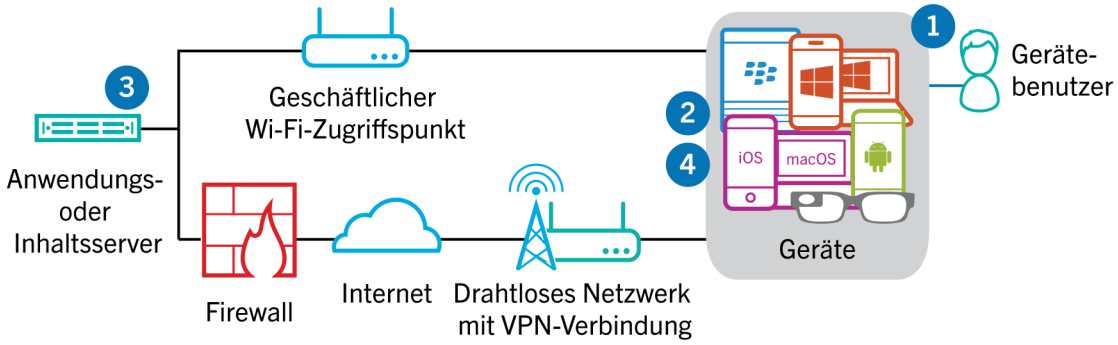


1. Das Gerät sendet eine HTTPS-Anforderung an den E-Mail-Server und fordert diesen auf, das Gerät zu benachrichtigen, wenn sich Elemente in den Ordnern ändern, die für die Synchronisierung konfiguriert sind. Die Anforderung wird über das VPN Ihres Unternehmens oder das Wi-Fi-Geschäftsnetzwerk an den 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.

Empfangen von Konfigurationsupdates für Geräte

Wenn Sie die Verwaltungskonsole zum Senden von Gerätebefehlen verwenden, wie Gerät sperren oder die geschäftlichen Daten löschen, oder wenn Sie andere Geräteverwaltungsaufgaben ausführen (Aktualisierungen von 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 das Gerät, dass ein Konfigurationsupdate aussteht. Außerdem rufen Geräte von BlackBerry UEM 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.

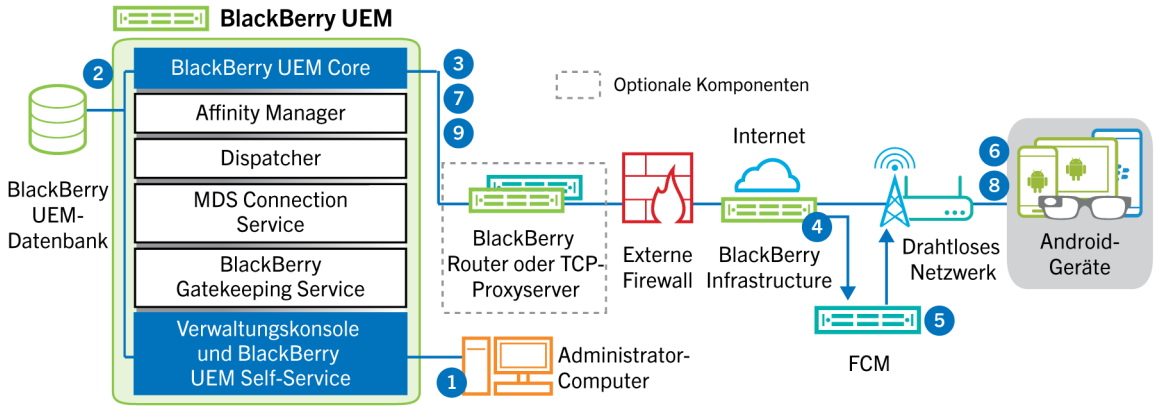
Auf Android-Geräten empfängt und schließt der BlackBerry UEM Client alle Konfigurationsupdates ab.

Auf iOS-Geräten zeigt die BlackBerry UEM Client-App den Status zur Einhaltung von Vorschriften und Konfigurationsinformationen für das Gerät an, wie Apps oder ihm zugewiesene Richtlinien. Der native MDM-Daemon auf dem Gerät empfängt und schließt alle Konfigurationsupdates ab, die an das Gerät gesendet wurden.

Auf Windows 10- und macOS-Geräten, die für die Aktivierung nicht den BlackBerry UEM Client erfordern, empfängt der native MDM-Daemon alle Konfigurationsupdates auf dem Gerät und schließt sie ab.

Auf BlackBerry 10-Geräten empfängt und schließt der Enterprise Management Agent alle Konfigurationsupdates ab.

Datenfluss: Empfangen von Konfigurationsupdates auf einem Android-Gerät



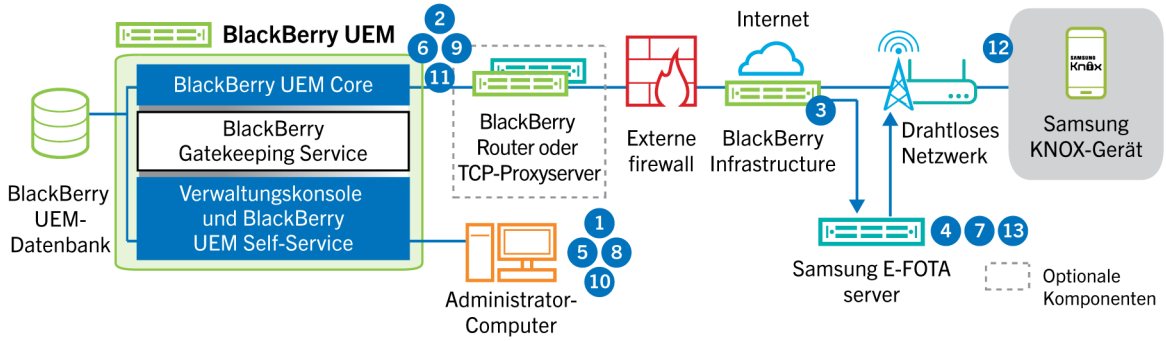
1. In der Verwaltungskonsole wird eine Aktion vorgenommen, die ein Konfigurationsupdate für ein Android-Gerät auslöst.
2. Updates werden in BlackBerry UEM angewendet und Objekte, die für das Gerät freigegeben werden müssen, werden identifiziert.
3. Der BlackBerry UEM Core kontaktiert die BlackBerry Infrastructure über den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, und die externe Firewall über Port 3101.
4. Die BlackBerry Infrastructure verwendet FCM, um Android-Geräte darüber zu benachrichtigen, dass ein Update aussteht.
5. GCM sendet eine Benachrichtigung an den BlackBerry UEM Client auf dem Android-Gerät mit der Aufforderung, Kontakt mit BlackBerry UEM Core aufzunehmen.
6. Der BlackBerry UEM Client kontaktiert den BlackBerry UEM Core auf Port 3101 auf der externen Firewall, um ausstehende Aktionen und Befehle anzufordern, die auf dem Gerät durchgeführt werden müssen.
7. Der BlackBerry UEM Core antwortet über die BlackBerry Infrastructure und den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, mit der Aktion der höchsten Priorität.

   IT-Administrationsbefehle wie das Löschen von Gerätedaten und das Sperren von Geräten werden vorrangig behandelt, gefolgt von Anforderungen zur Weiterleitung von Informationen über Geräte, installierte Apps usw. Der BlackBerry UEM Core sendet jeweils nur einen Befehl. Bei Bedarf enthält die Antwort zusätzliche Informationen.
8. Der BlackBerry UEM Client überprüft die Antwort, plant den zu verarbeitenden Befehl und wartet darauf, dass der Befehl ausgeführt wird. Der BlackBerry UEM Client sendet über die BlackBerry UEM Core eine Antwort an den BlackBerry Infrastructure, um den Befehlsstatus zu aktualisieren. Der Status zeigt an, ob der Befehl erfolgreich ausgeführt wurde, und gibt bei einem Fehler eine Fehlermeldung aus.
9. Wenn mehrere Aktionen oder Befehle für das Gerät ausstehen, antwortet der BlackBerry UEM Core über die BlackBerry Infrastructure mit der Aktion der höchsten Priorität. Wenn keine Aktionen oder Befehle für das Gerät ausstehen, leitet der BlackBerry UEM Core einen Leerlaufbefehl weiter.

   Schritte 7 bis 9 werden wiederholt, bis alle ausstehenden Aktionen oder Befehle auf dem Gerät durchgeführt wurden.

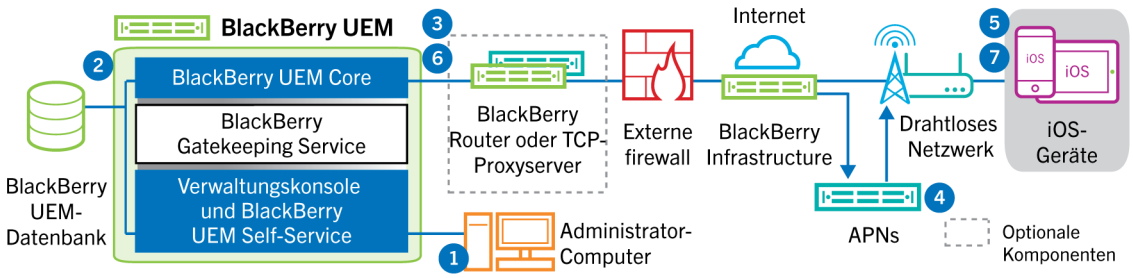
Datenfluss: Firmware auf Samsung Knox-Geräten aktualisieren

In diesem Datenfluss wird beschrieben, wie Daten übertragen werden, wenn Sie Samsung Enterprise Firmware Over the Air verwenden, um zu steuern, wann Firmware-Aktualisierungen von Samsung auf Geräte installiert werden. Weitere Informationen finden Sie in der Dokumentation für Administratoren unter Steuern der Softwareversionen, die auf Geräten installiert sind.



1. Ein Administrator fügt eine Samsung E-FOTA-Kunden-ID und einen Lizenzschlüssel zu BlackBerry UEM hinzu.
2. Die BlackBerry UEM Core sendet die Lizenzinformationen über eine TLS-Verbindung an BlackBerry Infrastructure.
3. Die BlackBerry Infrastructure stellt eine TLS-Verbindung zu den Samsung E-FOTA-Servern her und stellt die Kunden-ID und den Lizenzschlüssel bereit.
4. Der E-FOTA-Server überprüft die Informationen und gibt Lizenzinformationen über die BlackBerry Infrastructure an BlackBerry UEM Core zurück.
5. Ein Administrator erstellt ein SR-Anforderungsprofil für ein Gerät und legt ein Samsung-Gerätemodell, Sprache und einen Mobilfunkanbieter für eine neue Firmware-Regel für Samsung-Geräte fest.
6. Das BlackBerry UEM Core stellt über BlackBerry Infrastructure eine TLS-Verbindung zum E-FOTA-Server her und sendet die angegebenen Kriterien an den E-FOTA-Server.
7. Der E-FOTA-Server überprüft die Kriterien und gibt Lizenzinformationen über die BlackBerry Infrastructure an BlackBerry UEM Core zurück.
8. Der Administrator speichert das neue SR-Anforderungsprofil des Geräts.
9. Das BlackBerry UEM Core stellt über BlackBerry Infrastructure eine TLS-Verbindung zum E-FOTA-Server her und sendet das Profil an die Samsung-Cloud.
10. Der Administrator weist einem oder mehreren Benutzern das SR-Anforderungsprofil des Geräts zu.
11. BlackBerry UEM sendet das Profil an das BlackBerry UEM Client auf dem Samsung-Gerät des Benutzers.
12. Das Samsung-Gerät meldet sich beim E-FOTA-Server an.
13. Wenn eine Firmware-Aktualisierung verfügbar ist, die den im SR-Anforderungsprofil des Geräts angegebenen Parametern entspricht, sendet der E-FOTA-Server die Aktualisierung an das Gerät.

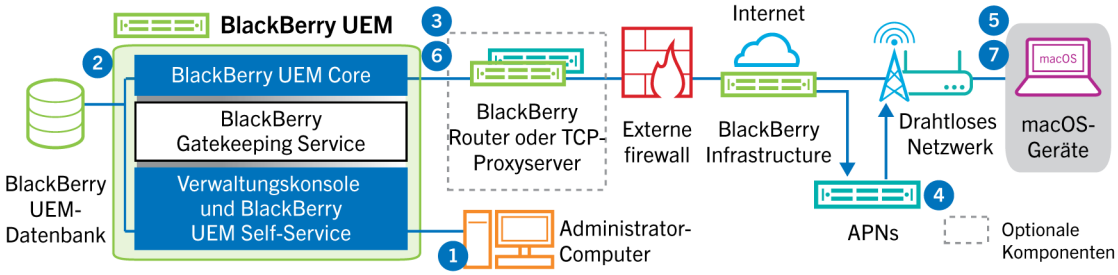
Datenfluss: Empfangen von Konfigurationsupdates auf einem iOS-Gerät



1. In der Verwaltungskonsole wird eine Aktion vorgenommen, die ein Konfigurationsupdate für ein iOS-Gerät auslöst. Beispiel: Sie aktualisieren die IT-Richtlinie oder weisen dem Benutzerkonto ein neues Profil oder eine neue App zu.
2. Updates werden in BlackBerry UEM angewendet und Objekte, die für das Gerät freigegeben werden müssen, werden identifiziert.
3. Die BlackBerry UEM Core führt die folgenden Aktionen aus:
   a. Er kontaktiert die BlackBerry Infrastructure über den BlackBerry Router oder den TCP-Proxyserver, falls installiert, und die externe Firewall über Port 3101.
   b. Er sendet eine Anfrage über die BlackBerry Infrastructure an den APNs, um das Gerät darüber zu benachrichtigen, dass ein Update aussteht.
4. Die APNs senden eine Benachrichtigung an den nativen MDM-Daemon auf dem iOS-Gerät, um den BlackBerry UEM Core zu kontaktieren.
5. Wenn der native MDM-Daemon auf dem iOS-Gerät die Benachrichtigung empfängt, kontaktiert er den BlackBerry UEM Core auf Port 3101 der externen Firewall, die über den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, geleitet wird, um ausstehende Aktionen abzurufen.
6. Der BlackBerry UEM Core antwortet mit der Aktion der höchsten Priorität. Geräteaktionen wird Priorität gewährt, z. B. „Gerätedaten löschen“ und „Gerät sperren“. Der BlackBerry UEM Core sendet jeweils nur einen Befehl. Bei Bedarf enthält die Antwort zusätzliche Informationen. Wenn keine Aktionen oder Befehle für das Gerät ausstehen, leitet BlackBerry UEM Core einen Leerlaufbefehl an das Gerät weiter.
7. Der native MDM-Daemon auf dem iOS-Gerät führt folgende Aktionen aus:
   a. Er überprüft die Antwort von BlackBerry UEM Core, plant den zu verarbeitenden Befehl und wartet darauf, dass der Befehl ausgeführt wird.
   b. Er sendet eine Antwort an BlackBerry UEM Core zur Aktualisierung des Befehlsstatus. Der Status zeigt an, ob der Befehl erfolgreich ausgeführt wurde, und gibt bei einem Fehler eine Fehlermeldung aus.

   Schritte 6 bis 7 werden wiederholt, bis alle ausstehenden Aktionen oder Befehle auf dem Gerät durchgeführt wurden.

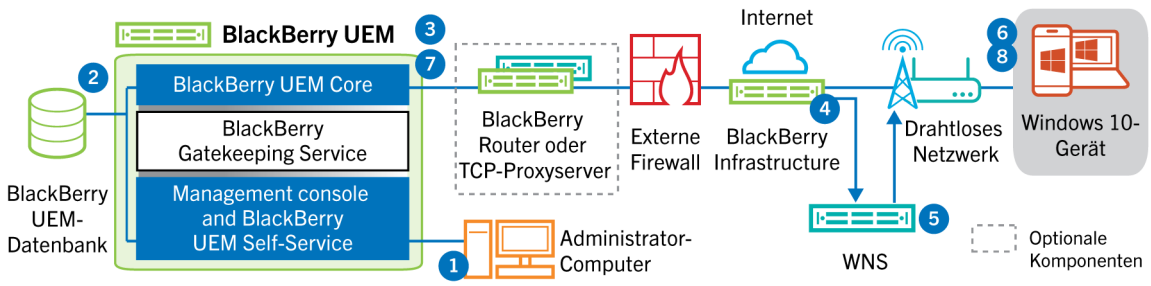
Datenfluss: Empfangen von Konfigurationsupdates auf einem macOS-Gerät



1. In der Verwaltungskonsole wird eine Aktion vorgenommen, die ein Konfigurationsupdate für ein macOS-Gerät auslöst. Beispiel: Sie aktualisieren die IT-Richtlinie oder weisen dem Benutzerkonto ein neues Profil oder eine neue App zu.
2. Updates werden in BlackBerry UEM angewendet und Objekte, die für das Gerät freigegeben werden müssen, werden identifiziert.
3. Die BlackBerry UEM Core führt die folgenden Aktionen aus:
   a. Er kontaktiert die BlackBerry Infrastructure über den BlackBerry Router oder den TCP-Proxyserver, falls installiert, und die externe Firewall über Port 3101.
   b. Er sendet eine Anfrage über die BlackBerry Infrastructure an den APNs, um das Gerät darüber zu benachrichtigen, dass ein Update aussteht.
4. APNs sendet eine Benachrichtigung an das Gerät mit der Aufforderung, Kontakt mit BlackBerry UEM Core aufzunehmen.
5. Wenn das Gerät die Benachrichtigung empfängt, kontaktiert es den BlackBerry UEM Core auf Port 3101 auf der externen Firewall, die über den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, geleitet wird, um ausstehende Aktionen abzurufen.
6. Steht ein Update für das Gerät aus, antwortet der BlackBerry UEM Core mit der Aktion der höchsten Priorität. Geräteaktionen wird Priorität gewährt, z. B. „Gerätedaten löschen“ und „Gerät sperren“. Bei Bedarf enthält die Antwort zusätzliche Informationen. Wenn keine Aktionen oder Befehle für das Gerät ausstehen, leitet BlackBerry UEM Core eine leere Nachricht an das Gerät weiter.
7. Das Gerät führt die folgenden Aktionen aus:
   a. Er überprüft die Antwort von BlackBerry UEM Core, plant den zu verarbeitenden Befehl und wartet darauf, dass der Befehl ausgeführt wird.
   b. Er sendet eine Antwort an BlackBerry UEM Core zur Aktualisierung des Befehlsstatus. Der Status zeigt an, ob der Befehl erfolgreich ausgeführt wurde, und gibt bei einem Fehler eine Fehlermeldung aus.

   Schritte 6 bis 7 werden wiederholt, bis alle ausstehenden Aktionen oder Befehle auf dem Gerät durchgeführt wurden.

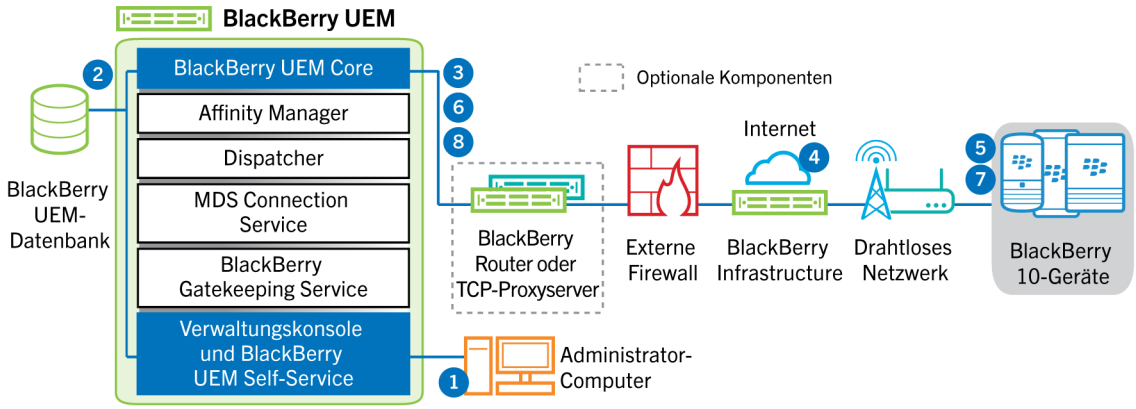
Datenfluss: Empfangen von Konfigurationsupdates auf einem Windows 10-Gerät



1. In der Verwaltungskonsole wird eine Aktion vorgenommen, die ein Konfigurationsupdate für ein Windows 10-Gerät auslöst. Beispiel: Sie aktualisieren die IT-Richtlinie oder weisen dem Benutzerkonto ein neues Profil oder eine neue App zu.
2. Updates werden in BlackBerry UEM angewendet und Objekte, die für das Gerät freigegeben werden müssen, werden identifiziert.
3. Der BlackBerry UEM Core kontaktiert die BlackBerry Infrastructure über den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, und die externe Firewall über Port 3101.
4. Die BlackBerry Infrastructure verwendet WNS, um das Gerät darüber zu benachrichtigen, dass ein Update aussteht.
5. WNS sendet eine Benachrichtigung an das Gerät mit der Aufforderung, Kontakt mit dem BlackBerry UEM Core aufzunehmen.
6. Wenn das Gerät die Benachrichtigung empfängt, kontaktiert es den BlackBerry UEM Core auf Port 3101 auf der externen Firewall, die über den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, geleitet wird, um ausstehende Aktionen abzurufen.
7. Steht ein Update für das Gerät aus, antwortet der BlackBerry UEM Core mit der Aktion der höchsten Priorität. Geräteaktionen wird Priorität gewährt, z. B. „Gerätedaten löschen“ und „Gerät sperren“. Bei Bedarf enthält die Antwort zusätzliche Informationen. Wenn keine Aktionen oder Befehle für das Gerät ausstehen, leitet BlackBerry UEM Core eine leere Nachricht an das Gerät weiter.
8. Das Gerät prüft die Antwort, plant die Verarbeitung des Befehls und wartet auf dessen Durchführung. Das Gerät sendet eine Antwort an den BlackBerry UEM Core zur Aktualisierung des Befehlsstatus. Der Status zeigt an, ob der Befehl erfolgreich ausgeführt wurde, und gibt bei einem Fehler eine Fehlermeldung aus.

   Schritte 7 bis 8 werden wiederholt, bis keine Aktionen oder Befehle auf dem Gerät mehr ausstehen.

Datenfluss: Empfangen von Konfigurationsupdates auf einem BlackBerry 10-Gerät



1. In der Verwaltungskonsole wird eine Aktion vorgenommen, die ein Konfigurationsupdate für das Gerät auslöst. Beispiel: Sie aktualisieren die IT-Richtlinie oder weisen dem Benutzerkonto ein neues Profil oder eine neue App zu.
2. Updates werden in BlackBerry UEM angewendet und Objekte, die für das Gerät freigegeben werden müssen, werden identifiziert.
3. Der BlackBerry UEM Core benachrichtigt die BlackBerry Infrastructure darüber, dass ein Update für das Gerät vorhanden ist. Die Benachrichtigung wird über den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, und die externe Firewall über Port 3101 geleitet.
4. Die BlackBerry Infrastructure benachrichtigt den Enterprise Management Agent auf dem Gerät darüber, dass ein Update vorhanden ist.
5. Der Enterprise Management Agent auf dem Gerät sendet eine Anfrage an BlackBerry UEM Core, um ausstehende Aktionen zu ermitteln, die auf dem Gerät durchgeführt werden müssen. Diese Abfrage wird über die BlackBerry Infrastructure und den BlackBerry Router, falls installiert, an den BlackBerry UEM Core geleitet.
6. Der BlackBerry UEM Core antwortet über die BlackBerry Infrastructure und den BlackBerry Router oder den TCP-Proxy-Server, falls installiert, mit der Aktion der höchsten Priorität.

   IT-Administrationsbefehle wie das Löschen von Gerätedaten und das Sperren von Geräten werden vorrangig behandelt, gefolgt von Anforderungen zur Weiterleitung von Informationen über Geräte, installierte Apps usw. Der BlackBerry UEM Core sendet jeweils nur einen Befehl. Bei Bedarf enthält die Antwort zusätzliche Informationen.
7. Der Enterprise Management Agent auf dem Gerät empfängt die Konfigurationsupdates und wendet die neue oder aktualisierte Konfiguration auf das Gerät an. Der Enterprise Management Agent sendet über die BlackBerry UEM Core eine Antwort an den BlackBerry Infrastructure, um den Befehlsstatus zu aktualisieren. Der Status zeigt an, ob der Befehl erfolgreich ausgeführt wurde, und gibt bei einem Fehler eine Fehlermeldung aus.
8. Wenn mehrere Aktionen oder Befehle für das Gerät ausstehen, antwortet der BlackBerry UEM Core über die BlackBerry Infrastructure mit der Aktion der höchsten Priorität. Wenn keine Aktionen oder Befehle für das Gerät ausstehen, leitet der BlackBerry UEM Core einen Leerlaufbefehl weiter.

   Schritte 6 bis 8 werden wiederholt, bis alle ausstehenden Aktionen oder Befehle auf dem Gerät durchgeführt wurden.

Rechtliche Hinweise

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

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

SOFERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDEN 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 MANGELNDEN 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 JEGLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEGLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE, VERSCHÄRFTEN SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE,

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada