BlackBerry UEM

Verwalten von Android-Geräten

Verwalten

12.16

Contents

Verwalten von Android-Geräten

BlackBerry UEM ermöglichen eine präzise Verwaltung der Verbindung von Android-Geräten mit dem Netzwerk, der aktivierten Funktionen und der verfügbaren Apps. Unabhängig davon, ob Ihre Geräte Eigentum Ihres Unternehmens oder Ihrer Benutzer sind, können Sie mobilen Zugriff auf die Informationen Ihres Unternehmens gewähren und diese gleichzeitig vor allen Personen schützen, die keinen Zugriff haben sollten.

In diesem Handbuch wird erläutert, welche Optionen Sie zur Verwaltung von Android-Geräten haben und wie Sie die verfügbaren Funktionen im Einzelnen nutzen können.

Verwalten von Wearables

Sie können bestimmte Wearables auf Android-Basis in BlackBerry UEM aktivieren und verwalten. Wearable-Geräte, wie z. B. intelligente Brillen, ermöglichen den berührungslosen Zugriff auf visuelle Informationen, wie z. B. Benachrichtigungen, Schritt-für-Schritt-Anleitungen, Bilder und Videos, die Nutzung von Sprachsteuerung und GPS-Navigation oder das Scannen von Barcodes.

BlackBerry UEM unterstützt die folgenden Wearables:

- Vuzix M300 Smart Glasses

Um Wearables zu verwalten, folgen Sie den Anweisungen für Android-Geräte. Die folgenden BlackBerry UEM-Funktionen werden für Wearable-Geräte unterstützt:

- Geräteaktivierung mit einem QR Code
- IT-Richtlinien
- WLAN, VPN, unternehmensweite Konnektivität, Konformitäts- und Zertifikatprofile
- BlackBerry Secure Connect Service
- Gerätebefehle
- App-Verwaltung
- Gerätegruppen
- Standortdienste

Wearable-Geräte verwenden den BlackBerry UEM Client für die Aktivierung. Sie können Wearable-Geräte mit einem QR-Code anstelle eines Aktivierungskennworts aktivieren.

Was Sie auf Android-Geräten steuern können

BlackBerry UEM bietet alle Tools, die Sie zur Steuerung der Funktionen benötigen, die mit Android-Geräten verwaltet werden können. Darüber hinaus bietet es Funktionen, mit denen Sie Gerätebenutzern einen sicheren Zugriff auf geschäftliche Ressourcen gewähren können, ohne das Gerät vollständig verwalten zu müssen.

Steuerungsebene	Beschreibung
Nicht verwaltete Geräte Privatsphäre des Benutzers-Aktivierungen	Sie können ein Gerät auf BlackBerry UEM mit dem Aktivierungstyp „Privatsphäre des Benutzers“ aktivieren, um einen sicheren Zugriff auf geschäftliche Ressourcen ohne Verwaltung des Geräts zu ermöglichen. Diese Option wird häufig für BYOD-Geräte verwendet. Diese Aktivierungen ermöglichen es Benutzern, über VPN mithilfe von BlackBerry 2FA auf Ihr Netzwerk zuzugreifen, Dateien sicher mithilfe von BlackBerry Workspaces freizugeben und BlackBerry Dynamics-Apps wie BlackBerry Work und BlackBerry Access zu installieren, um auf geschäftliche E-Mails und Ihr geschäftliches Intranet zuzugreifen.
Verwaltete Geräte mit einem Arbeitsprofil Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)-Aktivierungen	Android Enterprise-Geräte können verwaltet werden, ermöglichen aber durch Erstellung eines Arbeitsprofils auf dem Gerät, das geschäftliche und persönliche Daten voneinander trennt, die private Nutzung. Diese Option hält für die privaten Daten des Benutzers im persönlichen Profil den Datenschutz aufrecht, ermöglicht Ihnen jedoch die Verwaltung der Geschäftsdaten über Befehle und IT-Richtlinienregeln. Sie können geschäftliche Apps, wie z. B. BlackBerry Dynamics-Apps, auf dem Gerät verwalten. Sie können Daten vom Gerät bereinigen. Dies gilt jedoch nicht für persönliche Daten. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Diese Option wird häufig für unternehmenseigene, persönlich aktivierte Geräte (COPE, Corporate-Owned, Personally Enabled) und BYOD-Geräte verwendet.
Vollständig verwaltete Geräte mit einem Arbeitsprofil Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)-Aktivierungen	Android Enterprise-Geräte können vollständig verwaltet werden, ermöglichen jedoch in gewissem Umfang eine private Nutzung, und zwar durch Erstellung eines Arbeitsprofils auf dem Gerät, das geschäftliche und persönliche Daten trennt, Ihrem Unternehmen jedoch die vollständige Kontrolle über das Gerät und die Möglichkeit einer Bereinigung aller Daten auf dem Gerät sichert. Einige IT-Richtlinienregeln können separat auf das geschäftliche und das persönliche Profil angewendet werden. Sie können geschäftliche Apps, wie z. B. BlackBerry Dynamics-Apps, auf dem Gerät verwalten. Sie können auf dem Gerät gesendete und empfangene SMS, MMS und Telefonanrufe protokollieren. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Diese Option wird häufig für COPE-Geräte verwendet.

Steuerungsebene	Beschreibung
Vollständig verwaltete Geräte Nur geschäftlicher Bereich (Android Enterprise)-Aktivierungen	Android Enterprise-Geräte können vollständig verwaltet werden und haben ein geschäftliches Profil, aber kein persönliches Profil. Diese Option ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Sie können geschäftliche Apps, wie z. B. BlackBerry Dynamics-Apps, auf dem Gerät verwalten. Sie können auf dem Gerät gesendete und empfangene SMS, MMS und Telefonanrufe protokollieren. Alle Daten auf dem Gerät werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise ein Kennwort, geschützt. Diese Option wird häufig für unternehmenseigene, rein geschäftliche Geräte (COBO, Corporate-Owned, Business Only) verwendet.
Geräteadministration MDM-Steuerelemente-Aktivierungen	Sie können Geräte mit Android 9.x (und älter) über Befehle und IT-Richtlinienregeln verwalten. Es wird kein separater geschäftlicher Bereich auf dem Gerät erzeugt, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten. Um die Sicherheit geschäftlicher Daten sicherzustellen, können Sie BlackBerry Dynamics-Apps installieren. Diese Aktivierungsart wird für Android 10-Geräte nicht unterstützt. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community. Sie können Gerätegruppen und Konformitätsprofile verwenden, um festzulegen, was mit Geräten mit „MDM-Steuerelemente“-Aktivierungen geschieht, die auf Android 10 aktualisiert werden. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

Android Enterprise bietet vollständige Unterstützung für die Verwaltung von Android-Geräten, einschließlich der folgenden Funktionen:

- Durchsetzung von Kennwortanforderungen
- Steuerung von Gerätefunktionen mithilfe von IT-Richtlinien (z. B. Deaktivierung der Kamera oder Bluetooth)
- Erzwingung von Kompatibilitätsregeln
- Erstellung von Wi-Fi- und VPN-Verbindungsprofilen (mit Proxy)
- Synchronisierung von E-Mails, Kontakten und Kalendern mit Geräten
- Versenden von Zertifizierungsstellen- und Clientzertifikaten an Geräte, um Authentifizierung und S/MIME zu ermöglichen
- Verwaltung erforderlicher und zugelassener öffentlicher und interner Apps
- Ortung und Schutz verlorener oder gestohlener Geräte

Android Enterprise-Geräte, die mit BlackBerry UEM aktiviert werden, unterstützen darüber hinaus zusätzliche Steuerelemente, die nur für Geräte mit der Samsung Knox Platform for Enterprise und BlackBerry-Geräte mit Android verfügbar sind.

BlackBerry UEM unterstützt nicht nur Samsung Knox Platform for Enterprise, sondern außerdem Geräte mit Samsung Knox Workspace-Aktivierungen. Samsung Knox-Aktivierungsarten werden in zukünftigen Versionen nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 54614 unter https://support.blackberry.com/community.

Hinweis: Einige Funktionen und BlackBerry Dynamics-Apps sind nicht für alle Lizenzstufen verfügbar. Weitere Informationen zu den verfügbaren Lizenzen finden Sie in der Dokumentation zur Lizenzierung.

Schritte zum Verwalten von Android-Geräten

Schritt	Aktion
1	Installieren und konfigurieren Sie BlackBerry UEM gemäß Installationsanweisungen.
2	Wenn Ihr Unternehmen Android Enterprise-Geräte verwalten möchte, konfigurieren Sie ein verwaltetes Google Play-Konto oder eine Verbindung zu Ihrer Google Cloud- oder G Suite-Domäne.
3	Konfigurieren Sie die IT-Richtlinien für die Geräte. Weisen Sie Benutzergruppen oder einzelnen Benutzern IT-Richtlinien zu.
4	Konfigurieren Sie Profile für die Geräte. Weisen Sie Benutzergruppen oder einzelnen Benutzern Profile zu.
5	Geben Sie die Apps an, die Geräte installieren können oder müssen.
6	Aktivieren Sie Geräte.
7	Verwalten und überwachen Sie Geräte.

Unterstützen von Android Enterprise-Aktivierungen

Die Art und Weise, wie Benutzer Android Enterprise-Geräte aktivieren, hängt von verschiedenen Faktoren ab, einschließlich der Android-Betriebssystemversion, wie viel Kontrolle Ihr Unternehmen über die Geräte der Benutzer haben möchte und wie Ihr Unternehmen die Google-Dienste nutzt. Ihr Unternehmen kann auf folgende Weise mit Google-Diensten interagieren:

Verbindung zu Google-Diensten	Beschreibung
Verwaltete Google Play-Konten	BlackBerry UEM ist nicht mit einer Google-Domäne verbunden. Sie können verwaltete Google Play-Konten verwenden, um Benutzern das Herunterladen und Installieren von geschäftlichen Apps mit Google Play zu ermöglichen. Weitere Informationen finden Sie Unterstützung von Android Enterprise-Aktivierungen mithilfe verwalteter Google Play-Konten
G Suite-Domäne	Ihr Unternehmen verfügt über eine G Suite-Domäne, die alle G Suite-Dienste wie Gmail, Google Calendar und Google Drive unterstützt. Weitere Informationen finden Sie Unterstützen von Android Enterprise-Aktivierungen mit einer G Suite-Domäne
Google Cloud-Domäne	Ihr Unternehmen verfügt über eine Google Cloud-Domäne, die Benutzern verwaltete Google-Konten bereitstellt. Ihr Unternehmen nutzt keine G Suite-Dienste wie Gmail, Google Calendar und Google Drive für die E-Mail-, Kalender- und Datenverwaltung Ihres Unternehmens. Weitere Informationen finden Sie Unterstützen von Android Enterprise-Aktivierungen mit einer Google Cloud-Domäne
Keine Google-Dienste	Aufgrund der Sicherheitsrichtlinien Ihres Unternehmens ist es nicht möglich Google-Dienste zu verwenden. Weitere Informationen finden Sie Unterstützung von Android Enterprise-Geräten ohne Zugriff auf Google Play

Weitere Informationen zum Konfigurieren von BlackBerry UEM für die Verbindung mit einer Google-Domäne oder zur Verwendung verwalteter Google Play-Konten finden Sie in der Dokumentation zur lokalen Konfiguration oder in der Dokumentation zur Cloud-Konfiguration.

Unterstützung von Android Enterprise-Aktivierungen mithilfe verwalteter Google Play-Konten

Wenn Ihr Organisation keine Google-Domäne hat oder wenn Sie BlackBerry UEM nicht mit Ihrer Google-Domäne verbinden möchten, können Sie Android Enterprise-Geräte für die Nutzung verwalteter Google Play-Konten aktivieren. Mithilfe verwalteter Google Play-Konten können Sie interne Apps zu Google Play hinzufügen, die nur von entsprechend aktivierten Benutzergeräten heruntergeladen werden können. Weitere Informationen zu verwalteten Google Play-Konten finden Sie unter https://support.google.com/googleplay/work/.

Wenn Sie verwaltete Google Play-Konten mit BlackBerry UEM verwenden, können Sie die Verbindung zwischen BlackBerry UEM und Google über ein beliebiges Google- oder Gmail-Konto herstellen. Es werden keine

personenbezogenen Daten über Ihre Benutzer an Google gesendet. Sobald Sie eine Verbindung zwischen BlackBerry UEM und Google hergestellt haben, können Sie Benutzern die Aktivierung von Android Enterprise-Geräten und das Herunterladen geschäftlicher Apps mit Google Play gestatten. Informationen dazu, wie Sie BlackBerry UEM konfigurieren müssen, damit Android Enterprise-Geräte unterstützt werden, finden Sie in der Dokumentation zur lokalen Konfiguration oder in der Dokumentation zur UEM Cloud-Konfiguration.

Unterstützen von Android Enterprise-Aktivierungen mit einer G Suite-Domäne

Wenn Sie BlackBerry UEM für eine Verbindung mit einer G Suite-Domäne konfiguriert haben, müssen Sie die folgenden Aufgaben ausführen, bevor Benutzer Android Enterprise-Geräte aktivieren können.

Bevor Sie beginnen: Konfigurieren von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten Informationen dazu, wie Sie BlackBerry UEM konfigurieren müssen, damit Android Enterprise-Geräte unterstützt werden, finden Sie in der Dokumentation zur lokalen Konfiguration oder in der Dokumentation zur UEM Cloud-Konfiguration.

1. Erstellen Sie in der G Suite-Domäne Benutzerkonten für die Android-Benutzer.
2. Wählen Sie in der G Suite-Domäne die Einstellung **EMM-Richtlinie erzwingen** aus.

   Diese Einstellung ist für Geräte mit den Aktivierungsarten Nur geschäftlicher Bereich und Geschäftlich und persönlich – vollständige Kontrolle erforderlich und wird für Geräte mit anderen Aktivierungsarten dringend empfohlen. Wenn diese Einstellung nicht ausgewählt ist, können Benutzer ein verwaltetes Google-Konto auf dem Gerät hinzufügen, um auf geschäftliche Apps außerhalb des geschäftlichen Profils zuzugreifen.
3. Wenn Sie den Aktivierungstyp Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle zuweisen möchten, wählen Sie in der G Suite-Domäne die Einstellung **EMM-Richtlinie erzwingen** aus.
4. Erstellen Sie in BlackBerry UEM lokale Benutzerkonten für die Android-Benutzer. Die E-Mail-Adressen der einzelnen Konten müssen mit denen der zugehörigen G Suite-Konten übereinstimmen.
5. Stellen Sie sicher, dass die Benutzer das Kennwort für ihr G Suite-Konto kennen.
6. Weisen Sie in BlackBerry UEM Benutzern, Benutzergruppen oder Gerätegruppen ein E-Mail-Profil und Produktivitäts-Apps zu.

Unterstützen von Android Enterprise-Aktivierungen mit einer Google Cloud-Domäne

Wenn Sie BlackBerry UEM für eine Verbindung mit einer Google Cloud-Domäne konfiguriert haben, müssen Sie die folgenden Aufgaben ausführen, damit Benutzer Geräte mithilfe von Android Enterprise aktivieren können.

Bevor Sie beginnen: Konfigurieren Sie BlackBerry UEM so, dass Android Enterprise unterstützt wird. Wenn Sie BlackBerry UEM für die Verbindung mit einer Google Cloud-Domäne konfigurieren, müssen Sie auswählen, ob BlackBerry UEM Benutzerkonten in dieser Domäne erstellen kann. Diese Auswahl hat Auswirkungen auf die Aufgaben, die Sie durchführen müssen, bevor Benutzer Android Enterprise-Geräte aktivieren können. Informationen dazu, wie Sie BlackBerry UEM konfigurieren müssen, damit Android Enterprise-Geräte unterstützt werden, finden Sie in der Dokumentation zur lokalen Konfiguration oder in der Dokumentation zur UEM Cloud-Konfiguration.

1. Fügen Sie in BlackBerry UEM Verzeichnis-Benutzerkonten für die Android Enterprise-Benutzer hinzu.
2. Wenn Sie nicht zulassen, dass BlackBerry UEM in Ihrer Google Cloud-Domäne Benutzerkonten erstellt, müssen Sie in der Google Cloud-Domäne und in BlackBerry UEM Benutzerkonten erstellen. Führen Sie eine der folgenden Aktionen aus:

- Erstellen Sie in der Google Cloud-Domäne Benutzerkonten für die Android Enterprise-Benutzer. Die E-Mail-Adressen der jeweiligen Konten müssen mit denen der zugehörigen BlackBerry UEM-Benutzerkonten übereinstimmen. Stellen Sie sicher, dass Ihre Android Enterprise-Benutzer das Kennwort für ihre Google Cloud-Konten kennen.
- Synchronisieren Sie mithilfe von Google Apps Directory Sync Ihre Google Cloud-Domäne mit Ihrem Unternehmensverzeichnis. Wenn Sie dies tun, müssen Sie keine Benutzerkonten in Ihrer Google Cloud-Domäne manuell erstellen.

3. Wenn Sie den Aktivierungstyp Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle zuweisen möchten, wählen Sie in der Google Cloud-Domäne die Einstellung **EMM-Richtlinie erzwingen** aus.

   Diese Einstellung ist für Geräte mit den Aktivierungsarten Nur geschäftlicher Bereich und Geschäftlich und persönlich – vollständige Kontrolle erforderlich und wird für Geräte mit anderen Aktivierungsarten dringend empfohlen. Wenn diese Einstellung nicht ausgewählt ist, können Benutzer ein verwaltetes Google-Konto auf dem Gerät hinzufügen, um auf geschäftliche Apps außerhalb des geschäftlichen Profils zuzugreifen.
4. Weisen Sie in BlackBerry UEM Benutzern, Benutzergruppen oder Gerätegruppen ein E-Mail-Profil und Produktivitäts-Apps zu.

Unterstützung von Android Enterprise-Geräten ohne Zugriff auf Google Play

Um Geräte ohne Zugriff auf Google Play zu aktivieren, müssen Benutzer den neuesten BlackBerry UEM Client von einer anderen Quelle herunterladen. Je nach Betriebssystemversion und Aktivierungsart stehen verschiedene Methoden zum Herunterladen des UEM Client zur Verfügung:

- Bei Geräten, die mit den Aktivierungsarten Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle aktiviert werden, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden, bevor UEM Client installiert wird. Um den Download-Speicherort auf dem Gerät anzugeben, können Sie den Speicherort in einem QR Code angeben, den der Benutzer scannt, um die Aktivierung zu starten oder zuzulassen, dass das Gerät Download-Informationen über NFC erhält (z. B. durch Tippen auf einen NFC-Sticker oder ein anderes Gerät).
  - Weitere Informationen zur Angabe des UEM Client-Speicherorts in einem QR Code finden Sie unter Standardmäßige Geräteaktivierungseinstellungen.
  - Informationen zum Programmieren eines NFC-Sticker finden Sie unter Programmieren eines NFC-Stickers zur Aktivierung von Geräten.
  - Informationen, um mit der BlackBerry UEM Enroll-App auf einem zweiten Gerät UEM Client-Download-Anweisungen über NFC bereitzustellen, finden Sie in der UEM Enroll-Dokumentation. Um diese Methode zu verwenden, muss die App BlackBerry UEM Enroll auf einem Gerät mit Android 9 installiert sein, und das zu aktivierende Gerät muss mit Android 9 oder einer früherer Version arbeiten.
- Geräte, die mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz aktiviert werden, müssen nicht zuerst auf die Werkseinstellungen zurückgesetzt werden. Bei diesen Geräten können Benutzer den BlackBerry UEM Client von der BlackBerry-Download-Website oder einem anderen verfügbaren Speicherort herunterladen, nachdem die Einrichtung des vorkonfigurierten Geräts abgeschlossen ist.

Um die APK-Datei der neuesten UEM Client- oder UEM Enroll-App herunterzuladen, besuchen Sie support.blackberry.com/community, und lesen Sie Artikel 42607.

Anweisungen zum Aktivieren von Android Enterprise-Geräten finden Sie unter Aktivieren von Android-Geräten

Anforderungen

Wenn Sie Geräte aktivieren möchten, die keinen Zugriff auf Google Play haben, überprüfen Sie Folgendes:

Anforderungen	Beschreibung
BlackBerry UEM - Umgebung	• **Integration in Android Enterprise**: Sie müssen UEM nicht in Android Enterprise integrieren, wenn nur Geräte unterstützt werden sollen, die keinen Zugriff auf Google Play haben. Wenn jedoch Geräte mit und ohne Zugriff auf Google Play unterstützt werden sollen, müssen Sie die UEM-Umgebung in Android Enterprise integrieren.
Standardeinstellungen für die Geräteaktivierung	Wenn Sie den Speicherort von UEM Client in einen QR-Code aufnehmen möchten, überprüfen Sie die folgenden Standardeinstellungen für die Geräteaktivierung: • Wählen Sie die Optionen **Zulassen, dass der QR-Code den Speicherort der Quelldatei der UEM-Client-App enthält** und **Standardspeicherort verwenden** aus. Über diese Optionen können Benutzer den QR-Code in der Aktivierungs-E-Mail scannen, um den UEM Client von der BlackBerry-Download-Website herunterzuladen. Diese Optionen sind nur verfügbar, wenn Ihre UEM-Umgebung in Android Enterprise integriert ist.
Aktivierungsprofileinstellungen	Überprüfen Sie die folgenden Einstellungen im Aktivierungsprofil: • Deaktivieren Sie die Option **Google Play-Konto zu Arbeitsbereich hinzufügen**. Diese Option ist nur verfügbar, wenn Ihre UEM-Umgebung in Android Enterprise integriert ist. • Wenn Sie BlackBerry Secure Connect Plus aktivieren möchten, wählen Sie die Option **Bei der Aktivierung von Android Enterprise-Geräten UEM-Sonderfunktionen wie BlackBerry Secure Connect Plus aktivieren**. Sie müssen die BlackBerry Connectivity-App als interne App hochladen und sie Benutzern zuweisen.
IT-Richtlinienregeln	Überprüfen Sie für Benutzer, denen die Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) zugewiesen ist, in der IT-Richtlinie Folgendes: • Aktivieren Sie die IT-Richtlinienregel **Installation von Apps, die nicht von Google Play stammen, zulassen**, um die Installation von Apps außerhalb von Google Play zuzulassen.

Anforderungen	Beschreibung
Nicht-BlackBerry Dynamics-Apps	Fügen Sie Nicht-BlackBerry Dynamics-Apps als interne Apps zu UEM hinzu, und ordnen Sie sie den entsprechenden Benutzern zu. 1. Rufen Sie die APK-Dateien der Apps ab, die Sie zuweisen möchten. Um beispielsweise die neueste Version der BlackBerry Connectivity-App herunterzuladen, besuchen Sie das BlackBerry-Portal myAccount. 2. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**. 3. Klicken Sie auf > **Interne Apps**. 4. Klicken Sie auf **Durchsuchen**, und wählen Sie die APK-Datei aus. 5. Wählen Sie im Feld **Senden an** die Option **Alle Android-Geräte** aus. 6. Deaktivieren Sie die Option **App in Google-Domäne veröffentlichen**. 7. Klicken Sie auf **Hinzufügen**. 8. Wiederholen Sie die zuvor genannten Schritte für jede App, die Sie hinzufügen möchten. 9. Weisen Sie die Apps Benutzern zu. Die App-Verfügbarkeit muss auf **Erforderlich** gesetzt sein.
BlackBerry Dynamics-Apps	Laden Sie für BlackBerry Dynamics-Apps die interne App-Quelldatei hoch, und weisen Sie die App Benutzern zu. Führen Sie die folgenden Schritte aus, um interne Apps auf Geräten, die keinen Zugriff auf Google Play haben, zu installieren oder zu aktualisieren: 1. Rufen Sie die APK-Dateien der BlackBerry Dynamics-Apps ab, die Sie zuweisen möchten. Um beispielsweise BlackBerry Work herunterzuladen, besuchen Sie support.blackberry.com/community, und lesen Sie Artikel 42607. 2. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**. 3. Klicken Sie auf eine BlackBerry Dynamics-App (z. B. BlackBerry Work). 4. Klicken Sie auf die Registerkarte **Android**. 5. Klicken Sie auf **Quelldatei für interne App hinzufügen**. 6. Klicken Sie auf **Durchsuchen**, und wählen Sie die APK-Datei aus. 7. Klicken Sie auf **Hinzufügen**. 8. Klicken Sie auf **Speichern**. 9. Wiederholen Sie die zuvor genannten Schritte für jede App, die Sie hinzufügen möchten. 10. Weisen Sie die Apps Benutzern zu. Die App-Verfügbarkeit muss auf **Erforderlich** gesetzt sein.
BlackBerry UEM Client-App aktualisieren	Um die UEM Client-App auf Geräten zu aktualisieren, müssen Benutzer die neueste Version der APK-Datei manuell herunterladen und installieren. Weitere Informationen finden Sie unter support.blackberry.com/community in Artikel 42607.

Weitere Informationen zur Unterstützung von Android Enterprise-Geräten ohne Zugriff auf Google Play finden Sie unter support.blackberry.com/community in Artikel 57492.

Programmieren eines NFC-Stickers zur Aktivierung von Geräten

Benutzer können den BlackBerry UEM Client herunterladen und die Geräteaktivierung starten, indem sie auf ein NFC-Tag oder einen NFC-Sticker tippen. Diese Methode ist eine Option zum Aktivieren von Geräten mit Nur geschäftlicher Bereich (Android Enterprise) und Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise), die keinen Zugriff auf Google Play haben.

Damit Benutzer Geräte mit dieser Methode aktivieren können, programmieren Sie einen Drittanbieter-NFC-Sticker mit den Werten, die erforderlich sind, um das Gerät anzuweisen, den UEM Client herunterzuladen und mit der Aktivierung zu beginnen.

Bevor Sie beginnen: Folgende Elemente sind erforderlich:

- NFC-Tag oder -Sticker
- Eine Methode zur Programmierung des Stickers, z. B. eine Android-App, die NFC-Sticker lesen und auf diese schreiben kann.

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > Externe Integration > Android Enterprise**.
2. Klicken Sie unter **NFC-Registrierung** auf **Weitere Informationen**.
3. Öffnen Sie auf einem Gerät mit einer App, die Daten auf NFC-Sticker schreiben kann, die App, und lassen Sie zu, dass die App eine Verbindung mit dem Sticker herstellt, den Sie programmieren möchten. Fügen Sie dann die folgenden Einstellungen hinzu:
   a) Setzen Sie den NFC-Datentyp auf `Benutzerdefiniert`.
   b) Setzen Sie den Inhaltstyp auf `application/com.android.managedprovisioning`
   c) Kopieren Sie die Details aus dem Textfeld in der Verwaltungskonsole in der App in das Feld **Konfiguration**.
4. Lassen Sie die Einstellungen in den Sticker schreiben.

Nachdem das Programm auf den Sticker geschrieben wurde, sollten Benutzer in der Lage sein, mit einem neuen Gerät oder einem auf die Werkseinstellungen zurückgesetzten Gerät auf den Sticker zu tippen, um den UEM Client herunterzuladen und die Aktivierung zu starten.

Festlegen der standardmäßigen Aktivierungseinstellungen

Sie können die Standardeinstellungen für die Geräteaktivierung festlegen, einschließlich der Standardzeit, die ein Aktivierungskennwort gültig bleibt, bevor es abläuft, der Länge der automatisch generierten Kennwörter, die an Benutzer gesendet werden, ob QR Code für die Aktivierung verwendet werden können, und anderer Optionen.

Weitere Informationen zu den Standardeinstellungen für die Geräteaktivierung finden Sie unter Standardmäßige Geräteaktivierungseinstellungen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen**.
2. Klicken Sie auf **Standards der Aktivierung**.
3. Geben Sie unter **Geräteaktivierungsstandards** das Aktivierungskennwort und QR Code-Optionen an.
4. Wenn Sie Android-Geräte bis Version 9.0 verwalten und die Aktivierungsart MDM-Steuerelemente verwenden möchten, aktivieren Sie das Kontrollkästchen **Aktivierungsart MDM-Steuerelemente für Android-Geräte aktivieren**, um MDM-Steuerelemente der Liste der Aktivierungsarten im Aktivierungsprofil hinzuzufügen.

   Diese Option ist standardmäßig aktiviert, wenn BlackBerry UEM von einer früheren Version aktualisiert wurde. Wenn diese Option aktiviert ist, können Sie sie nicht deaktivieren.
5. Wählen Sie **QR-Codes für das Entsperren von BlackBerry Dynamics-Apps verwenden**, damit Benutzer BlackBerry Dynamics-Apps mit einem QR Code aktivieren können. Weitere Informationen finden Sie unter Generieren von Zugriffsschlüsseln, Aktivierungskennwörtern oder QR Code für BlackBerry Dynamics-Apps

6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Registrierung mit BlackBerry Infrastructure einschalten**, um zu ändern, wie Benutzer ihre Mobilgeräte aktivieren. Wenn Sie diese Option deaktivieren, werden die Benutzer bei der Geräteaktivierung aufgefordert, die Serveradresse für BlackBerry UEM anzugeben. Weitere Informationen finden Sie unter Aktivieren der Benutzerregistrierung mit der BlackBerry Infrastructure.
7. Um eine Liste genehmigter Geräte-IDs zu importieren oder zu exportieren, navigieren Sie zur CSV-Datei Ihres Unternehmens, die eine Liste genehmigter Geräte-IDs enthält. Weitere Informationen finden Sie unter Importieren oder Exportieren einer Liste genehmigter Geräte-IDs.
8. Klicken Sie auf **Speichern**.

Standardmäßige Geräteaktivierungseinstellungen

Einstellung	Beschreibung
Ablauf des Aktivierungszeitraums	Sie können die Standardzeit festlegen, die ein Aktivierungskennwort oder QR Code gültig bleiben soll, bevor es abläuft. Der Wert muss zwischen 1 Minute und 30 Tagen liegen.
Aktivierungszeitraum endet nach der Aktivierung des ersten Geräts	Diese Einstellung gibt an, ob das Aktivierungskennwort oder QR Code nach der Aktivierung eines Geräts abläuft.
QR Codes für Geräteaktivierung zulassen	Diese Einstellung legt fest, ob ein QR Code in die Aktivierungs-E-Mail-Nachricht aufgenommen und in BlackBerry UEM Self-Service angezeigt werden kann. Benutzer können den QR Code scannen, um die Geräteaktivierung zu starten. Wenn diese Option nicht aktiviert ist, ist die Option zum Senden eines QR Codes nicht in der Vorlage für die Aktivierungs-E-Mail enthalten.
Zulassen, dass der QR Code das Aktivierungskennwort enthält	Diese Einstellung legt fest, ob der QR Code das Aktivierungskennwort beinhaltet. Wenn diese Option ausgewählt ist, müssen Benutzer nach dem Scannen eines QR-Codes für die Aktivieren eines Geräts kein separates Kennwort eingeben.
Zulassen, dass QR Code den Speicherort der UEM Client-App-Quelldatei enthält	Diese Einstellung legt fest, ob der QR Code-Code einen Speicherort enthält, über den die UEM Client-App-Quelldatei (APK) auf das Gerät heruntergeladen werden kann. Diese Einstellung ist nur für die Aktivierung von Android Enterprise-Geräten mit den Aktivierungsarten Nur geschäftlicher Bereich und Geschäftlich und persönlich – vollständige Kontrolle relevant. Geräte starten das Herunterladen und Installieren des BlackBerry UEM Clients durch Scannen des QR Codes.
Standardspeicherort verwenden	Wenn Sie zulassen, dass der QR Code den Speicherort der UEM Client-Quelldatei enthält, wählen Sie diese Option aus, um anzugeben, dass das Gerät die APK-Datei von der BlackBerry Download-Website erhalten soll.
Speicherort der Quelldatei für die UEM Client-App	Wenn Sie zulassen, dass der QR Code den Speicherort der UEM Client-Quelldatei enthält, gibt diese Einstellung den Speicherort an, von dem das Gerät die Datei herunterlädt. Sie können jeden Standort angeben, auf den das Gerät Zugriff hat, wenn es auf die Werkseinstellungen gesetzt ist.

Einstellung	Beschreibung
Verwendung von Microsoft Active Directory-Benutzername und -Kennwort zulassen	Für Geräte, die mit Samsung Knox Mobile Enrollment aktiviert wurden, gibt diese Einstellung auch an, ob Benutzer ihre Microsoft Active Directory-Anmeldeinformationen zum Aktivieren ihrer Geräte verwenden können.
Geräteaktivierte Benachrichtigung senden	Diese Einstellung gibt an, ob der Benutzer eine E-Mail-Benachrichtigung erhält, wenn ein Gerät aktiviert wurde.
Länge des automatisch generierten Aktivierungskennworts	Diese Einstellung legt die Anzahl der Zeichen für ein automatisch generiertes Kennwort fest. Der Wert muss zwischen 4 und 16 liegen.
Komplexität des automatisch generierten Kennworts	Diese Einstellung legt die Art der Zeichen für ein automatisch generiertes Kennwort fest. Kennwörter können die folgenden Arten von Zeichen enthalten: • Kleinbuchstaben • Großbuchstaben • Zahlen • Sonderzeichen oder Symbole
Aktivierungsart MDM-Steuerelemente für Android-Geräte aktivieren	Diese Einstellung legt fest, ob MDM-Steuerelemente in der Liste der Android-Aktivierungsarten im Aktivierungsprofil enthalten ist. Google unterstützt diese Aktivierungsart für Geräte mit Android 10 und höher nicht mehr. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community. Diese Option ist standardmäßig aktiviert, wenn BlackBerry UEM von einer früheren Version aktualisiert wurde. Wenn diese Option aktiviert ist, können Sie sie nicht deaktivieren.
QR-Codes für das Entsperren von BlackBerry Dynamics-Apps verwenden	Diese Einstellung legt fest, ob Benutzer BlackBerry Dynamics-Apps mit einem QR Code aktivieren können. Weitere Informationen finden Sie unter Generieren von Zugriffsschlüsseln, Aktivierungskennwörtern oder QR Code für BlackBerry Dynamics-Apps
Registrierung mit BlackBerry Infrastructure einschalten	Aktivieren oder deaktivieren Sie das Kontrollkästchen **Registrierung mit BlackBerry Infrastructure einschalten**, um zu ändern, wie Benutzer ihre iOS-, iPadOS-, macOS- und Android-Geräte aktivieren. Wenn Sie diese Option deaktivieren, werden die Benutzer bei der Aktivierung von Geräten aufgefordert, die Serveradresse für BlackBerry UEM anzugeben. Weitere Informationen finden Sie unter Aktivieren der Benutzerregistrierung mit der BlackBerry Infrastructure.

Steuerung von Android-Geräten mit einer IT-Richtlinie

BlackBerry UEM sendet eine IT-Richtlinie an jedes Gerät. Sie können eine Standard-IT-Richtlinie verwenden oder eigene IT-Richtlinien erstellen. Sie können so viele IT-Richtlinien erstellen, wie Sie für verschiedene Situationen und Benutzer benötigen, aber auf einem Gerät ist immer nur eine IT-Richtlinie aktiv.

Die IT-Richtlinienregeln für Android basieren auf den Funktionen des Geräts und den von Google und dem Gerätehersteller bereitgestellten Gerätekonfigurationsoptionen. Wenn Google neue Betriebssystem-Updates mit neuen Funktionen und Konfigurationsoptionen veröffentlicht, werden UEM bei der nächsten möglichen Gelegenheit neue IT-Richtlinienregeln hinzugefügt.

Sie können die durchsuchbare und sortierbare Tabelle der IT-Richtlinienregeln herunterladen. In der Tabelle werden alle in UEM verfügbaren Regeln sowie die zur Unterstützung der Regel gültigen Mindestanforderungen an das Betriebssystem dokumentiert.

Das Geräteverhalten, das Sie mit einer IT-Richtlinie steuern, umfasst die folgenden Optionen:

- Kennwortanforderungen an das Gerät
- Zulassen von Gerätefunktionen, wie z. B. Kamera und Bluetooth
- Zulassen, dass Apps in einem Profil auf Daten in einem anderen Profil zugreifen
- Einschränkung der Funktionen nur für Apps und Daten im geschäftlichen Profil

Weitere Informationen zum Senden von IT-Richtlinien an Geräte finden Sie in der Dokumentation für Administratoren.

Einrichten der Android Kennwortanforderungen

Es gibt vier Gruppen von IT-Richtlinienregeln für Android-Kennwörter. Welche Regeln Sie verwenden, hängt von der Aktivierungsart des Geräts ab, und davon, ob sie Anforderungen für das Gerätekennwort oder das Kennwort für den geschäftlichen Bereich festlegen.

Nachdem Sie Kennwortregeln in der IT-Richtlinie festgelegt haben, verwenden Sie ein Kompatibilitätsprofil, um die Kennwortanforderungen zu erzwingen.

Aktivierungsart	Unterstützte Kennwortregeln
Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) und Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der globalen Kennwortregeln fest. Verwenden Sie die Kennwortregeln für geschäftliche Profile zum Festlegen der Kennwortanforderungen für das geschäftliche Profil. Die Knox-Kennwortregeln werden vom Gerät ignoriert.
Nur geschäftlicher Bereich (Android Enterprise)	Legen Sie die Kennwortanforderungen für das Gerät mithilfe der globalen Kennwortregeln fest. Da das Gerät nur einen geschäftlichen Bereich besitzt, ist das Kennwort ebenfalls das Kennwort für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert.

Aktivierungsart	Unterstützte Kennwortregeln
MDM-Steuerelemente	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der globalen Kennwortregeln fest. Alle anderen Kennwortregeln werden vom Gerät ignoriert. **Hinweis:** Die Aktivierungsart MDM-Steuerelemente wird für Geräte mit Android 10 nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community.
MDM-Steuerelemente (Samsung Knox)	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der Knox MDM-Kennwortregeln fest. Alle anderen Kennwortregeln werden vom Gerät ignoriert.
Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)	Sie haben keine Kontrolle über das Gerätekennwort. Verwenden Sie die Kennwortregeln für Knox Premium – Workspace zum Festlegen der Kennwortanforderungen für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert. **Hinweis:** Die Samsung Knox-Aktivierungsarten werden in einer zukünftigen Version nicht mehr unterstützt. Geräte, die Knox Platform for Enterprise unterstützen, können über die Android Enterprise-Aktivierungsarten aktiviert werden. Weitere Informationen finden Sie in Artikel 54614 unter https://support.blackberry.com/community.
Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der Knox MDM-Kennwortregeln fest. Verwenden Sie die Kennwortregeln für Knox Premium – Workspace zum Festlegen der Kennwortanforderungen für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert.
Nur geschäftlicher Bereich (Samsung Knox)	Verwenden Sie die Kennwortregeln für Knox Premium – Workspace zum Festlegen der Kennwortanforderungen für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert.

Android: Globale Kennwortregeln

Die globalen Kennwortregeln legen die Gerätekennwortanforderungen für Geräte mit den folgenden Aktivierungsarten fest:

- Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)
- Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)
- Nur geschäftlicher Bereich (Android Enterprise)
- MDM-Steuerelemente (ohne Samsung Knox)

Hinweis: Die Aktivierungsart MDM-Steuerelemente wird für Geräte mit Android 10 nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community.

Regel	Beschreibung
Kennwortanforderungen	Legen Sie die Mindestanforderungen für das Kennwort fest. Sie können eine der folgenden Optionen auswählen: • Nicht festgelegt – kein Kennwort erforderlich • Eingabe erforderlich – der Benutzer muss ein Kennwort einrichten, wobei es keine Anforderungen an Länge oder Qualität gibt • Numerisch – das Kennwort muss mindestens eine Zahl enthalten • Alphabetisch – das Kennwort muss mindestens einen Buchstaben enthalten • Alphanumerisch – das Kennwort muss mindestens einen Buchstaben und eine Zahl enthalten • Komplex – Sie können bestimmte Anforderungen bezüglich verschiedener Zeichentypen festlegen
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor das Gerät bereinigt oder deaktiviert wird. Geräte mit der Aktivierungsart „MDM-Steuerelemente“ werden bereinigt. Geräte mit den Aktivierungsarten „Geschäftlich und persönlich – Benutzerdatenschutz“ und „Geschäftlich und persönlich – Benutzerdatenschutz (Premium)“ werden deaktiviert, und das Arbeitsprofil wird entfernt.
Maximale Inaktivitätszeit für Sperre	Legen Sie die maximale Anzahl der Minuten für die Benutzerinaktivität fest, nach deren Ablauf das Gerät und der geschäftliche Bereich gesperrt werden. Auf Android-Geräten mit einem geschäftlichen Profil wird auch der geschäftliche Bereich gesperrt. Benutzer können auf dem Gerät einen kürzeren Zeitraum festlegen. Diese Regel wird ignoriert, wenn kein Kennwort erforderlich ist.
Timeout für Kennwortablauf	Legen Sie fest, wie lange das Kennwort maximal verwendet werden kann. Nachdem die angegebene Zeit verstrichen ist muss der Benutzer ein neues Kennwort festlegen. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Einschränkung für Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter das Gerät maximal prüft, um zu verhindern, dass ein vorheriges numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.
Mindestlänge für Kennwort	Legen Sie die Mindestanzahl der Zeichen für ein numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort fest.
Benötigte Mindestanzahl der Großbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Großbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Kleinbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Kleinbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Buchstaben im Kennwort	Legen Sie die Mindestanzahl der Buchstaben fest, die ein komplexes Kennwort enthalten muss.

Regel	Beschreibung
Mindestanzahl von Nicht-Buchstaben in Kennwort	Legen Sie die Mindestanzahl von nicht alphabetischen Zeichen (Zahlen oder Symbole) fest, die ein komplexes Kennwort enthalten muss.
Erforderliche Mindestanzahl an Ziffern in Kennwort	Legen Sie die Mindestanzahl der Zahlenzeichen fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Symbole im Kennwort	Legen Sie die Mindestanzahl an nicht alphanumerischen Zeichen fest, die ein komplexes Kennwort enthalten muss.

Weitere Informationen zu den IT-Richtlinien für Kennwortregeln finden Sie in der Richtlinien-Referenztabelle.

Android: Kennwortregeln für geschäftliche Profile

Die Kennwortregeln für geschäftliche Profile legen die Kennwortanforderungen für den geschäftlichen Bereich von Geräten mit den folgenden Aktivierungsarten fest:

- Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)
- Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)

Regel	Beschreibung
Kennwortanforderungen	Geben Sie die Mindestanforderungen für das Kennwort für den geschäftlichen Bereich an. Sie können eine der folgenden Optionen auswählen: • Eingabe erforderlich – der Benutzer muss ein Kennwort einrichten, wobei es keine Anforderungen an Länge oder Qualität gibt • Numerisch – das Kennwort muss mindestens eine Zahl enthalten • Alphabetisch – das Kennwort muss mindestens einen Buchstaben enthalten • Alphanumerisch – das Kennwort muss mindestens einen Buchstaben und eine Zahl enthalten • Komplex – Sie können bestimmte Anforderungen bezüglich verschiedener Zeichentypen festlegen • Numerisch komplex – das Kennwort muss Zahlen ohne sich wiederholenden (4444) oder geordneten Zahlenfolgen (1234, 4321, 2468) enthalten • Biometrisch schwach – es ist eine biometrische Erkennungstechnologie mit niedriger Sicherheitsstufe für das Kennwort zulässig. Für BlackBerry-Geräte mit Android können Sie mithilfe der Regel für BlackBerry-Geräte „Unterschiedliches Kennwort für geschäftlichen Bereich und Gerät erzwingen“ unterschiedliche Kennwörter für den geschäftlichen Bereich und das Gerät erzwingen.
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort für den geschäftlichen Bereich eingeben darf, bevor das Gerät deaktiviert und das geschäftliche Profil entfernt wird.

Regel	Beschreibung
Maximale Inaktivitätszeit für Sperre	Legen Sie die maximal Anzahl der Minuten für die Benutzerinaktivität fest, bevor das Gerät und der geschäftliche Bereich gesperrt werden. Wenn Sie sowohl diese Regel als auch die globale Android-Regel „Maximaler Zeitraum der Inaktivität bis Sperre“ festlegen, werden das Gerät und der geschäftliche Bereich gesperrt, wenn einer der beiden Zeiträume abläuft. Benutzer können auf dem Gerät einen kürzeren Zeitraum festlegen.
Timeout für Kennwortablauf	Legen Sie fest, wie lange das Kennwort für den geschäftlichen Bereich maximal verwendet werden kann. Nachdem die angegebene Zeit verstrichen ist, muss der Benutzer ein neues Kennwort für den geschäftlichen Bereich festlegen. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Einschränkung für Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter für den geschäftlichen Bereich das Gerät maximal prüft, um zu verhindern, dass ein vorheriges numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.
Mindestlänge für Kennwort	Legen Sie die Mindestanzahl der Zeichen für ein numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort für den geschäftlichen Bereich fest.
Benötigte Mindestanzahl der Großbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Großbuchstaben fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Benötigte Mindestanzahl der Kleinbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Kleinbuchstaben fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Benötigte Mindestanzahl der Buchstaben im Kennwort	Legen Sie die Mindestanzahl der Buchstaben fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Mindestanzahl von Nicht-Buchstaben in Kennwort	Legen Sie die Mindestanzahl von nicht alphabetischen Zeichen (Zahlen oder Symbole) fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Erforderliche Mindestanzahl an Ziffern in Kennwort	Legen Sie die Mindestanzahl der Zahlenzeichen fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Benötigte Mindestanzahl der Symbole im Kennwort	Legen Sie die Mindestanzahl an nicht alphanumerischen Zeichen fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Unterschiedliches Kennwort für Arbeitsprofil und Gerät erzwingen	Legen Sie fest, ob Benutzer unterschiedliche Kennwörter für das Gerät und das geschäftliche Profil festlegen müssen. Wenn die Kennwörter identisch sind, wird durch Entsperren des Geräts das geschäftliche Profil entsperrt.

Weitere Informationen zu den IT-Richtlinien für Kennwortregeln finden Sie in der Richtlinien-Referenztabelle.

Steuern von Android-Geräten mithilfe von Profilen

BlackBerry UEM enthält mehrere Profile, mit denen Sie verschiedene Gerätefunktionen steuern können. Am häufigsten werden die folgenden Profile verwendet:

Profilname	Beschreibung	Konfigurieren von
Aktivierung	Gibt die Geräteaktivierungseinstellungen für Benutzer an, z. B. den Aktivierungstyp, die Methode oder die Anzahl und Typen der Geräte, die ein Benutzer aktivieren kann.	Erstellen eines Aktivierungsprofils
Wi-Fi	Gibt die Einstellungen für Geräte an, um eine Verbindung zu Ihrem geschäftlichen Wi-Fi-Netzwerk herzustellen.	Erstellen eines Wi-Fi-Profils
VPN	Gibt die Einstellungen für Geräte an, um eine Verbindung zu einem geschäftlichen VPN herzustellen.	Erstellen eines VPN-Profils
Proxy	Gibt an, wie Geräte einen Proxyserver für den Zugriff auf Webdienste im Internet oder in einem geschäftlichen Netzwerk verwenden.	Erstellen eines Proxy-Profils
E-Mail	Gibt an, wie Geräte eine Verbindung zum geschäftlichen E-Mail-Server herstellen und E-Mail-Nachrichten, Kalendereinträge und Terminplanerdaten synchronisieren. Wenn Sie BlackBerry Work auf Geräten installieren und konfigurieren, müssen Sie kein E-Mail-Profil einrichten.	Erstellen eines E-Mail-Profils
BlackBerry Dynamics	Ermöglicht Geräten den Zugriff auf BlackBerry Dynamics-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect.	Erstellen eines BlackBerry Dynamics-Profils
BlackBerry Dynamics-Verbindungen	Definiert die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.	Erstellen eines BlackBerry Dynamics-Verbindungsprofils
Konformität	Definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind, und legt entsprechende Durchsetzungsaktionen fest.	Erstellen eines Kompatibilitätsprofils
Enterprise-Konnektivität	Gibt an, ob Geräte BlackBerry Secure Connect Plus verwenden können.	BlackBerry Secure Connect Plus aktivieren

Profilname	Beschreibung	Konfigurieren von
Zertifizierungsstellenzer	Gibt ein Zertifizierungsstellenzertifikat an, das von Geräten verwendet werden kann, um vertrauenswürdige Verbindungen mit einem geschäftlichen Netzwerk oder einem Server herzustellen.	Erstellen eines Profils mit Zertifizierungsstellenzertifikat
Benutzeranmeldeinformatione	Legt fest, wie Geräte Clientzertifikate abrufen, die zur Authentifizierung bei einem geschäftlichen Netzwerk oder Server verwendet werden.	Erstellen eines Profils mit Benutzeranmeldeinformationen
SCEP	Gibt den SCEP-Server an, den Geräte verwenden, um ein Clientzertifikat abzurufen, das zur Authentifizierung bei einem geschäftlichen Netzwerk oder Server dient.	Erstellen eines SCEP-Profils

Weitere Informationen zum Senden von Profilen an Geräte finden Sie in der Dokumentation für Administratoren.

Profilreferenz – Android-Geräte

In der folgenden Tabelle sind alle BlackBerry UEM-Profile aufgeführt, die auf Android-Geräten unterstützt werden:

Profilname	Beschreibung	Konfigurieren
Richtlinie		
Aktivierung	Gibt die Geräteaktivierungseinstellungen für Benutzer wie den Aktivierungstyp sowie die Anzahl und Typen der Geräte an.	Erstellen eines Aktivierungsprofils
BlackBerry Dynamics	Ermöglicht Geräten den Zugriff auf BlackBerry Dynamics-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect.	Erstellen eines BlackBerry Dynamics-Profils
App-Sperrmodus	Geben Sie eine einzelne App an, die auf Geräten ausgeführt werden soll. Nur mit MDM aktivierte Samsung Knox-Geräte	Erstellen eines Profils für den App-Sperrmodus
Enterprise Management Agent	Gibt an, wann Geräte eine Verbindung mit BlackBerry UEM herstellen, um für die App oder Konfiguration Updates zu erhalten, wenn keine Push-Benachrichtigung verfügbar ist.	Erstellen eines Enterprise Management Agent-Profils
Konformität		
Konformität	Definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind, und legt entsprechende Durchsetzungsaktionen fest.	Erstellen eines Kompatibilitätsprofils

Profilname	Beschreibung	Konfigurieren
Konformität (BlackBerry Dynamics)	Dieses schreibgeschützte Profil zeigt die Konformitätseinstellungen an, die aus Good Control in eine lokale BlackBerry UEM-Umgebung importiert wurden.	Verwalten der BlackBerry Dynamics-Kompatibilitätsprofile
Gerätedienstanforderungen	Definiert die Softwareversionen, die auf Geräten installiert sein müssen, und legt einen Updatezeitraum für im Vordergrund laufende Apps fest.	Erstellen eines Profils für Gerätedienstanforderungen
E-Mail, Kalender und Kontakte		
E-Mail	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen E-Mail-Server herstellen und E-Mail-Nachrichten, Kalendereinträge und Terminplanerdaten mithilfe von Exchange ActiveSync oder IBM Notes Traveler synchronisieren.	Erstellen eines E-Mail-Profils
IMAP/POP3-E-Mail	Gibt an, wie Geräte eine Verbindung mit einem IMAP- oder POP3-Mailserver herstellen und wie E-Mail-Nachrichten synchronisiert werden.	Erstellen eines IMAP/POP3-E-Mail-Profils
Gatekeeping	Gibt die Microsoft Exchange-Server für das automatische Gatekeeping an.	Erstellen eines Gatekeeping-Profils
Netzwerke und Verbindungen		
Wi-Fi	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen WLAN-Netzwerk herstellen.	Erstellen eines Wi-Fi-Profils
VPN	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen VPN herstellen.	Erstellen eines VPN-Profils
Proxy	Gibt an, wie Geräte einen Proxyserver für den Zugriff auf Webdienste im Internet oder in einem geschäftlichen Netzwerk verwenden.	Erstellen eines Proxy-Profils
Enterprise-Konnektivität	Gibt an, wie Geräte mithilfe der Enterprise-Konnektivität eine Verbindung mit den Ressourcen Ihres Unternehmens herstellen können. Bei Android Enterprise- und Samsung Knox Workspace-Geräten gibt das Enterprise-Konnektivitätsprofil an, ob Geräte BlackBerry Secure Connect Plus verwenden können.	BlackBerry Secure Connect Plus aktivieren

Profilname	Beschreibung	Konfigurieren
BlackBerry Dynamics-Verbindungen	Definiert die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.	Erstellen eines BlackBerry Dynamics-Verbindungsprofils
BlackBerry 2FA	Ermöglicht den Einsatz der Zwei-Faktor-Authentifizierung für Benutzer und legt die Konfiguration der Funktionen für die Vorauthentifizierung und Wiederherstellung fest.	Erstellen eines BlackBerry 2FA-Profils
APN-Profil	Ermöglicht es Ihnen, APNs für Geräte festzulegen, die für die Verbindung mit Betreibern verwendet werden sollen.	Erstellen eines APN-Profils
Schutz		
Microsoft Intune-App-Schutz	Ermöglicht die Verwaltung von mit Microsoft Intune geschützten Apps.	Erstellen eines Microsoft Intune-App-Schutzprofils
Standortdienst	Ermöglicht Ihnen, den Standort von Geräten anzufordern und die ungefähren Standorte auf einer Karte anzuzeigen.	Erstellen eines Profils für die Standortbestimmung
Nicht stören	Ermöglicht das Blockieren von BlackBerry Work for Android-Benachrichtigungen außerhalb der Arbeitstage und -stunden, die Sie festlegen.	Erstellen Sie ein Nicht stören-Profil
Benutzerdefiniert		
Gerät	Ermöglicht die Konfiguration der Informationen, die auf Geräten angezeigt werden.	Erstellen eines Geräteprofils
Zertifikate		
Zertifizierungsstellenzertifikat	Gibt ein Zertifizierungsstellenzertifikat an, das von Geräten verwendet werden kann, um vertrauenswürdige Verbindungen mit einem geschäftlichen Netzwerk oder einem Server herzustellen.	Erstellen eines Profils mit Zertifizierungsstellenzertifikat
Freigegebenes Zertifikat	Gibt ein Clientzertifikat an, das Geräte für die Authentifizierung von Benutzern mit einem geschäftlichen Netzwerk oder Server verwenden können.	Erstellen eines Profils für ein freigegebenes Zertifikat

Profilname	Beschreibung	Konfigurieren
Benutzeranmeldeinformationen	Gibt die Zertifizierungsstellenverbindung an, die Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	Erstellen eines Profils mit Benutzeranmeldeinformationen
SCEP	Gibt den SCEP-Server an, den Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	Erstellen eines SCEP-Profils
CRL	Gibt die CRL-Konfigurationen an, die BlackBerry UEM zur Überprüfung des Status von Zertifikaten verwenden kann. Nur BlackBerry-Geräte, die von Android unterstützt werden	Erstellen eines CRL-Profils
Profil mit Zertifikatzuordnung	Gibt an, welche Kundenzertifikate Apps verwenden sollen	Erstellen eines Profils mit Zertifikatzuordnung

Verwalten von Apps auf Android-Geräten

Sie können eine Bibliothek mit Apps erstellen, die Sie auf Geräten verwalten und überwachen möchten. Bei Android Enterprise-Geräten können nur Apps, die Sie zulassen, im geschäftlichen Profil installiert werden. BlackBerry UEM bietet die folgenden Optionen für die Verwaltung von Apps auf Android-Geräten:

- Weisen Sie öffentliche Apps von Google Play auf Geräten als optional oder erforderlich zu.
- Sie können benutzerdefinierte Apps auf UEM hochladen und sie als optionale oder erforderliche Apps bereitstellen.
- Konfigurieren Sie App-Einstellungen wie Verbindungseinstellungen vor, wenn dies von der App zugelassen wird.
- Blockieren Sie den Zugriff von Benutzern auf Apps.
- Konfigurieren Sie öffentliche, ISV- und benutzerdefinierte BlackBerry Dynamics-Apps, um Benutzern den Zugriff auf geschäftliche Ressourcen zu ermöglichen.
- Verbinden Sie UEM mit Microsoft Intune, um die Intune-App-Schutzrichtlinien direkt in der UEM-Verwaltungskonsole festzulegen und Office 365-Apps bereitzustellen und zu verwalten.
- Zeigen Sie die Liste der auf den Geräten installierten persönlichen Apps an.
- Lassen Sie zu, dass Benutzer Apps bewerten und überprüfen für andere Benutzer in Ihrer Umgebung.

App-Verhalten auf Android Enterprise-Geräten

Auf Geräten mit BlackBerry Dynamics-Aktivierung wird der Katalog für geschäftliche Apps in BlackBerry Dynamics Launcher angezeigt, wenn Sie dem Benutzer die Berechtigung „Funktion – BlackBerry App Store“ zugewiesen haben. Weitere Informationen finden Sie unter Hinzufügen des Katalogs mit geschäftlichen Apps zu BlackBerry Dynamics Launcher.

Bei Android Enterprise-Geräten tritt folgendes Verhalten auf:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	Apps werden automatisch installiert.	Apps werden automatisch aktualisiert.	Apps werden automatisch vom Gerät entfernt.	Das Geschäftsprofil und zugewiesene geschäftliche Apps werden von dem Gerät entfernt.
Öffentliche Apps mit Verfügbarkeitsein „Optional“	Der Benutzer kann wählen, ob er die Apps installieren möchte. Die Apps werden in Google Play for Work angezeigt.	Google Play for Work benachrichtigt Benutzer über Aktualisierungen.	Apps werden automatisch vom Gerät entfernt.	Das Geschäftsprofil und zugewiesene geschäftliche Apps werden von dem Gerät entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“ gehostet in BlackBerry UEM	Wird nur für Nur geschäftlicher Bereich-Geräte unterstützt. Apps werden automatisch installiert.	Wird nur für Nur geschäftlicher Bereich-Geräte unterstützt. Apps werden automatisch installiert.	Apps werden automatisch vom Gerät entfernt.	Apps werden automatisch vom Gerät entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Optional“ gehostet in BlackBerry UEM	Der Benutzer kann wählen, ob er die Apps installieren möchte. Die Apps werden in Google Play for Work angezeigt.	Google Play for Work benachrichtigt Benutzer über Aktualisierungen.	Apps werden automatisch vom Gerät entfernt.	Das Geschäftsprofil und zugewiesene geschäftliche Apps werden von dem Gerät entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“ gehostet in Google Play	Apps werden automatisch auf dem Gerät installiert.	Google Play for Work benachrichtigt Benutzer über Aktualisierungen.	Apps werden automatisch vom Gerät entfernt.	Das Geschäftsprofil und zugewiesene geschäftliche Apps werden von dem Gerät entfernt.
Interne Apps mit Verfügbarkeitseinstellung „Optional“ gehostet in Google Play	Der Benutzer kann wählen, ob er die Apps installieren möchte. Die Apps werden in Google Play for Work angezeigt.	Google Play for Work benachrichtigt Benutzer über Aktualisierungen.	Apps werden automatisch vom Gerät entfernt.	Das Geschäftsprofil und zugewiesene geschäftliche Apps werden von dem Gerät entfernt.

Sie können das Aktualisierungsverhalten für Apps festlegen, die im Vordergrund im Profil für Gerätedienstanforderungen ausgeführt werden.

Aktivieren von Android-Geräten

Die Schritte, die Benutzer ausführen, um den BlackBerry UEM Client zu installieren und die Android-Geräteaktivierung einzuleiten, hängen von verschiedenen Faktoren ab, z. B. von der Android OS-Version, dem Gerätehersteller, der Art und Weise der Verwendung von Google-Diensten in Ihrer Organisation, der im Geräteaktivierungsprofil angegebenen Aktivierungsart und von den Präferenzen Ihres Unternehmens. Sie können Benutzern Anweisungen in der Aktivierungs-E-Mail bereitstellen, die BlackBerry UEM an Benutzer sendet. Weitere Informationen finden Sie unter E-Mail-Vorlagen.

Android Enterprise-Geräte unterstützen mehrere Methoden, die Benutzern das Starten des Aktivierungsprozesses ermöglichen:

Aktivierungsmethode	Beschreibung
Installieren des UEM Client aus Google Play	Geräte, die mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz aktiviert werden, müssen vor der Aktivierung nicht auf die Werkseinstellungen zurückgesetzt werden. Um diese Geräte zu aktivieren, können Benutzer den UEM Client von Google Play auf ihr Gerät herunterladen. Weitere Informationen finden Sie unter Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz.
Der Benutzer lädt den UEM Client von der BlackBerry-Download-Website herunter	In Situationen, in denen Android-Benutzer keinen Zugriff auf Google Play haben, um Geräte mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz zu aktivieren, können sie die UEM Client APK-Datei von der BlackBerry-Download-Website herunterladen. Alternativ können Sie die Datei von BlackBerry herunterladen und an einem Speicherort bereitstellen, auf den Ihre Benutzer Zugriff haben. Weitere Informationen finden Sie unter support.blackberry.com/community in Artikel 42607.
Domänenanmeldeinformationen für Google während der Geräteeinrichtung eingeben	Wenn BlackBerry UEM mit der G Suite- oder Google Cloud-Domäne Ihres Unternehmens verbunden ist und Benutzer ihre geschäftlichen Google-Anmeldedaten eingeben, lädt das Gerät den UEM Client herunter und beginnt mit dem Aktivierungsprozess, um Geräte zu aktivieren, denen die Aktivierungsart Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle zugewiesen ist. Weitere Informationen finden Sie unter Aktivieren eines Android Enterprise-Geräts, wenn BlackBerry UEM mit einer Google-Domäne verbunden ist.
Scannen eines QR Code, der den Speicherort für den UEM Client-Download enthält	BlackBerry UEM ermöglicht Ihnen, den Speicherort für den UEM Client in einen QR Code einzufügen, der in der Aktivierungs-E-Mail an Benutzer gesendet wird. Um Geräte zu aktivieren, denen die Aktivierungsart Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle zugewiesen ist, können Benutzer sieben Mal auf den Startbildschirm des Geräts tippen, um einen QR Code-Leser zu öffnen und den QR Code zu scannen. Einige Gerätehersteller unterstützen diese Funktion möglicherweise nicht. Weitere Informationen finden Sie unter Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle mithilfe eines verwalteten Google Play-Kontos.

Aktivierungsmethode	Beschreibung
Eingeben des Hashtags afw#BlackBerry während der Geräteeinrichtung	Wenn Ihr Unternehmen verwaltete Google Play-Konten für die Verbindung zu Google-Diensten verwendet, um Geräte mit der Aktivierungsart Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle zu aktivieren, können Benutzer auf dem Bildschirm, auf dem sie ihre Google-Anmeldeinformationen während der Geräteeinrichtung eingeben, stattdessen `afw#blackberry` eintippen, um den Download von UEM Client zu initiieren und den Aktivierungsprozess zu starten. Bei Android-Geräten ab Version 11 wird `afw#BlackBerry` nur für die Aktivierungsart Nur geschäftlicher Bereich unterstützt. Bei Android-Geräten mit den Versionen 8 und 9 wird `afw#blackberry` nicht mehr unterstützt. Weitere Informationen finden Sie unter Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Nur geschäftlicher Bereich mithilfe eines verwalteten Google Play-Kontos.
Auf einen NFC-Sticker oder ein sekundäres Gerät mit der BlackBerry UEM Enroll-App tippen, in der der Speicherort für den UEM Client-Download programmiert wurde	Sie können einen NFC-Sticker programmieren oder ein zweites Gerät einrichten, auf dem die UEM Enroll-App installiert ist. Um Geräte zu aktivieren, denen die Aktivierungsart Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle zugewiesen ist, können Benutzer auf den NFC-Sticker oder das sekundäre Gerät tippen, um den UEM Client-Download zu starten. Über das gleiche sekundäre Gerät oder den NFC-Sticker können Geräte für mehrere Benutzer aktiviert werden. Weitere Informationen finden Sie unter Aktivieren eines Android Enterprise-Geräts ohne Zugriff auf Google Play.
Android-Zero-Touch-Registrierung oder Samsung Knox Mobile Enrollment	Mit der Android-Zero-Touch-Registrierung können Sie eine große Anzahl von Android Enterprise-Geräten gleichzeitig bereitstellen. Knox Mobile Enrollment ermöglicht die Bereitstellung einer großen Anzahl von Samsung Knox-Geräten mit Android Enterprise-Aktivierungen. Um diese Option verwenden zu können, müssen Geräte beim Kauf von einem autorisierten Händler für die Zero-Touch-Registrierung oder Knox Mobile Enrollment bereitgestellt werden. Weitere Informationen finden Sie unter Konfigurieren der Unterstützung für die Android Zero-Touch-Registrierung oder Aktivieren von mehreren Geräten mit Knox Mobile Enrollment.

Jede Option zum Herunterladen des UEM Client s und Starten der Geräteaktivierung wird nur von bestimmten Aktivierungsarten unterstützt. Bei den Aktivierungsarten Nur geschäftlicher Bereich und Geschäftlich und persönlich – vollständige Kontrolle hängen die unterstützten Optionen zudem davon ab, wie Ihr Unternehmen die Google-Dienste verwendet.

Aktivierungsart	Geschäftlich und persönlich – Benutzer-Datenschutz	Geschäftlich und persönlich – vollständige Kontrolle			Nur geschäftlicher Bereich		
Methode		**Google-Domäne**	**Google Play – verwaltet**	**Kein Zugriff auf Google**	**Google-Domäne**	**Google Play – verwaltet**	**Kein Zugriff auf Google**
Installation von UEM Client über Google Play oder Benutzerdownload	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Anmeldedaten für die Google-Domäne	Ja	Ja	Nein	Nein	Ja	Nein	Nein
QR Code scannen	Nein	Ja	Ja	Ja	Ja	Ja	Ja
afw#blackberry-Hashtag	Nein	Nein	Android 10	Nein	Nein	Android 10 und höher	Nein
Tippen auf NFC-Sticker oder sekundäres Gerät	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Android-Zero-Touch-Registrierung/S Knox Mobile Enrollment	Nein	Ja	Ja	Ja	Ja	Ja	Ja

Aktivierungsarten: Android-Geräte

Für Android-Geräte können Sie mehrere Aktivierungsarten auswählen und ihnen eine Reihenfolge zuweisen, um sicherzustellen, dass BlackBerry UEM die am besten geeignete Aktivierungsart für dieses Gerät zuweist. Wenn Sie beispielsweise „Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)“ den ersten Rang und „Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)“ den zweiten zuweisen, wird für Geräte, die Samsung Knox Workspace unterstützen, die erste Aktivierungsart verwendet, und für Geräte, die dies nicht tun, die zweite.

Die Android-Aktivierungsarten sind in den folgenden Tabellen enthalten:

- Android Enterprise-Geräte
- Android-Geräte ohne geschäftliches Profil
- Samsung Knox Workspace-Geräte

Android Enterprise-Geräte

Die folgenden Aktivierungsarten gelten nur für Android Enterprise-Geräte.

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise mit geschäftlichem Profil)	Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit Befehlen und IT-Richtlinienregeln. Diese Aktivierungsart erstellt ein geschäftliches Profil auf dem Gerät, durch das geschäftliche und persönliche Daten voneinander getrennt werden. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Um BlackBerry Secure Connect Plus- und Knox Platform for Enterprise-Support zu aktivieren, müssen Sie die Option **Bei der Aktivierung von Android Enterprise-Geräten Premium UEM-Funktionen wie z. B. BlackBerry Secure Connect Plus freischalten** im Aktivierungsprofil auswählen. Die Benutzer müssen dem BlackBerry UEM Client keine Administratorberechtigungen erteilen.
Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil)	Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Diese Aktivierungsart erstellt ein geschäftliches Profil auf dem Gerät, durch das geschäftliche und persönliche Daten voneinander getrennt werden. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstütz die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in BlackBerry UEM-Protokolldateien. Nach der Aktivierung verfügen Geschäftlich und persönlich – vollständige Kontrolle-Geräte nur über einen begrenzten Satz vorinstallierter Standard-Apps, wie Kamera, Telefon und Einstellungen, im persönlichen Bereich. Die Liste der beibehaltenen vorinstallierten Apps hängt vom Gerätehersteller und der Betriebssystemversion ab. Um BlackBerry Secure Connect Plus- und Knox Platform for Enterprise-Support zu aktivieren, müssen Sie die Option **Bei der Aktivierung von Android Enterprise-Geräten Premium UEM-Funktionen wie z. B. BlackBerry Secure Connect Plus freischalten** im Aktivierungsprofil auswählen. Für diese Aktivierungsart muss das Gerät vor der Aktivierung auf die Werkseinstellungen zurückgesetzt werden. Wenn BlackBerry UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt. Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.

Aktivierungsart	Beschreibung
Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)	Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Bei dieser Aktivierungsart muss der Benutzer das Gerät vor der Aktivierung auf die Werkseinstellungen zurücksetzen. Es wird ein geschäftliches Profil und kein persönliches Profil installiert. Der Benutzer muss ein Kennwort für den Zugriff auf das Gerät erstellen. Alle Daten auf dem Gerät werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise ein Kennwort, geschützt. Während der Aktivierung installiert das Gerät BlackBerry UEM Client automatisch und gewährt Administratorberechtigungen. Benutzer können die Administratorberechtigungen nicht aufheben oder die App deinstallieren. Nach der Aktivierung verfügen Nur geschäftlicher Bereich-Geräte nur über einen begrenzten Satz vorinstallierter Standard-Apps, wie Kamera, Telefon und Einstellungen, sowie die Apps, deren Verfügbarkeit Sie als „Erforderlich“ festgelegt haben. Die Liste der beibehaltenen vorinstallierten Apps hängt vom Gerätehersteller und der Betriebssystemversion ab. Um BlackBerry Secure Connect Plus- und Knox Platform for Enterprise-Support zu aktivieren, müssen Sie die Option **Bei der Aktivierung von Android Enterprise-Geräten Premium UEM-Funktionen wie z. B. BlackBerry Secure Connect Plus freischalten** im Aktivierungsprofil auswählen. Für diese Aktivierungsart muss das Gerät vor der Aktivierung auf die Werkseinstellungen zurückgesetzt werden. Wenn BlackBerry UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt.

Android-Geräte ohne geschäftliches Profil

Die folgenden Aktivierungsarten gelten für alle Android-Geräte.

Aktivierungsart	Beschreibung
MDM-Steuerelemente	Diese Aktivierungsart ermöglicht die Verwaltung des Geräts über Befehle und IT-Richtlinienregeln. Es wird kein separater geschäftlicher Bereich auf dem Gerät erzeugt, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten. **Hinweis:** Die Aktivierungsart 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. Wenn ein Gerät Knox MDM unterstützt, wendet diese Aktivierungsart die Knox MDM IT-Richtlinienregeln an. Wenn Sie Knox-MDM-Richtlinienregeln nicht anwenden möchten, deaktivieren Sie das Kontrollkästchen **Samsung KNOX auf Samsung-Geräten aktivieren, denen die Aktivierungsart „MDM-Steuerelemente“ zugewiesen ist**. Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.

Aktivierungsart	Beschreibung
Privatsphäre des Benutzers	Mithilfe der Privatsphäre des Benutzers-Aktivierungsart können Sie die grundlegende Steuerung von Geräten ermöglichen, einschließlich der Verwaltung geschäftlicher Apps, und gleichzeitig sicherstellen, dass die persönlichen Daten des Benutzers privat bleiben. Bei dieser Aktivierungsart ist kein separater Container auf dem Gerät installiert. Um die Sicherheit geschäftlicher Daten sicherzustellen, können Sie BlackBerry Dynamics-Apps installieren. Mit Privatsphäre des Benutzers aktivierte Geräte können Dienste wie Find my Phone und Root Detection nutzen. Administratoren können jedoch keine Geräterichtlinien steuern. Sie können außerdem die Privatsphäre des Benutzers-Aktivierungsart verwenden, um Chrome-OS-Geräte zu aktivieren, damit Sie Android BlackBerry Dynamics-Apps installieren und verwalten können.
Geräteregistrierung nur für BlackBerry 2FA	Diese Aktivierungsart unterstützt die BlackBerry 2FA-Lösung für Geräte, die nicht von BlackBerry UEM verwaltet werden. Diese Aktivierungsart bietet keine Geräteverwaltung oder Steuerelemente, gestattet Geräten jedoch, die BlackBerry 2FA-Funktion zu verwenden. Um diese Aktivierungsart zu verwenden, müssen Sie Benutzern zudem das BlackBerry 2FA-Profil zuweisen. Wenn ein Gerät aktiviert ist, können Sie begrenzte Geräteinformationen in der Verwaltungskonsole anzeigen. Außerdem können Sie das Gerät über einen Befehl deaktivieren. Diese Aktivierungsart wird nur für Microsoft Active Directory-Benutzer unterstützt. Weitere Informationen finden Sie in der Dokumentation zu BlackBerry 2FA.

Samsung Knox Workspace-Geräte

Die folgenden Aktivierungsarten gelten nur für Samsung-Geräte, die Knox Workspace unterstützen.

Hinweis: Samsung Knox-Aktivierungsarten werden in einer zukünftigen Version nicht mehr unterstützt. Geräte, die Knox Platform for Enterprise unterstützen, können über die Android Enterprise-Aktivierungsarten aktiviert werden. Weitere Informationen finden Sie in Artikel 54614 unter https://support.blackberry.com/community.

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Benutzer-Datenschutz - (Samsung Knox)	Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit Befehlen und IT-Richtlinienregeln. Diese Aktivierungsart unterstützt die Knox MDM IT-Richtlinienregeln nicht. Die Aktivierungsart erstellt einen separaten geschäftlichen Bereich, und der Benutzer muss ein Kennwort einrichten, um auf diesen zuzugreifen. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Der Benutzer muss außerdem ein Kennwort für die Bildschirmsperre erstellen, um das gesamte Gerät zu schützen, und wird den USB-Fehlerbehebungsmodus nicht nutzen können. Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)	Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und die Knox MDM- sowie Knox Workspace IT-Richtlinienregeln. Die Aktivierungsart erstellt einen separaten geschäftlichen Bereich, und der Benutzer muss ein Kennwort einrichten, um auf diesen zuzugreifen. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstütz die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in BlackBerry UEM-Protokolldateien. Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.
Nur geschäftlicher Bereich - (Samsung Knox)	Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und die Knox MDM- sowie Knox Workspace IT-Richtlinienregeln. Diese Aktivierungsart entfernt den persönlichen Bereich und installiert einen geschäftlichen Bereich. Der Benutzer muss ein Kennwort für den Zugriff auf das Gerät erstellen. Alle Daten auf dem Gerät werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstütz die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in BlackBerry UEM-Protokolldateien. Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.

Erstellen von Aktivierungsprofilen

Mithilfe von Aktivierungsprofilen können Sie steuern, wie die Geräte aktiviert und verwaltet werden. Ein Aktivierungsprofil gibt an, wie viele Geräte und welche Gerätetypen ein Benutzer aktivieren kann, und welche Aktivierungsart für den jeweiligen Gerätetyp verwendet werden soll.

Sie können Aktivierungsarten verwenden, um zu konfigurieren, wie viel Kontrolle Sie über aktivierte Geräte haben. Vielleicht möchten Sie die vollständige Kontrolle über ein Gerät, das Sie einem Benutzer bereitstellen. Vielleicht möchten Sie sicherstellen, dass sie keine Kontrolle über die persönlichen Daten eines Geräts haben, das einem Benutzer gehört und das er zur Arbeit mitbringt.

Das zugewiesene Aktivierungsprofil gilt nur für Geräte, die der Benutzer aktiviert, nachdem Sie ihm das Profil zugewiesen haben. Geräte, die bereits aktiviert sind, werden nicht automatisch aktualisiert, um dem neuen oder aktualisierten Aktivierungsprofil zu entsprechen.

Wenn Sie in BlackBerry UEM einen Benutzer hinzufügen, wird dem Benutzerkonto das Standard-Aktivierungsprofil zugewiesen. Sie können das Standard-Aktivierungsprofil den Anforderungen entsprechend ändern, oder Sie können ein benutzerdefiniertes Aktivierungsprofil erstellen und dieses Benutzern oder Benutzergruppen zuweisen.

Erstellen eines Aktivierungsprofils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinie > Aktivierung**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.

5. Geben Sie im Feld **Anzahl der Geräte, die ein Benutzer aktivieren kann** die maximale Anzahl von Geräten ein, die der Benutzer aktivieren kann.
6. Wählen Sie in der Dropdown-Liste **Geräteeigentümer** die Standardeinstellung für den Geräteeigentümer aus.
   - Wenn einige Benutzer persönliche Geräte und einige Benutzer geschäftliche Geräte aktivieren, wählen Sie **Nicht angegeben** aus.
   - Wählen Sie **Geschäftlich** aus, wenn die meisten Benutzer geschäftliche Geräte aktivieren.
   - Wählen Sie **Persönlich** aus, wenn die meisten Benutzer ihre persönlichen Geräte aktivieren.
7. Wählen Sie optional einen Organisationshinweis in der Dropdown-Liste **Organisationshinweis zuweisen** aus. Wenn Sie einen Organisationshinweis zuordnen, müssen Benutzer, die iOS-, iPadOS-, macOS oder Windows 10-Geräte aktivieren möchten, die Mitteilung akzeptieren, um den Aktivierungsvorgang abzuschließen.
8. Wählen Sie im Abschnitt **Gerätetypen, die Benutzer aktivieren können** die entsprechenden Geräte-OS-Typen aus. Gerätetypen, die Sie nicht auswählen, werden im Aktivierungsprofil nicht berücksichtigt, und Benutzer können diese Geräte nicht aktivieren.
9. Führen Sie die folgenden Aktionen für jeden Gerätetyp durch, der im Aktivierungsprofil enthalten ist:
   a) Klicken Sie auf die Registerkarte für den Gerätetyp.
   b) Wählen Sie in der Dropdown-Liste **Gerätemodell-Einschränkungen** eine der folgenden Optionen aus:
      - **Keine Einschränkungen**: Benutzer können jedes Gerätemodell aktivieren.
      - **Ausgewählte Gerätemodelle zulassen**: Benutzer können nur die von Ihnen angegebenen Gerätemodelle aktivieren. Verwenden Sie diese Option, um die zulässigen Geräte nur auf einige Modelle zu beschränken.
      - **Ausgewählte Gerätemodelle nicht zulassen**: Benutzer können die von Ihnen angegebenen Gerätemodelle nicht aktivieren. Verwenden Sie diese Option, um die Aktivierung einiger Gerätemodelle oder Geräte bestimmter Hersteller zu blockieren.

      Wenn Sie die Gerätemodelle einschränken, die Benutzer aktivieren können, klicken Sie auf **Bearbeiten**, um die Geräte auszuwählen, die Sie zulassen oder einschränken möchten, und klicken Sie dann auf **Speichern**.
   c) Wählen Sie in der Dropdown-Liste **Zugelassene Mindestversion** die OS-Version aus, die als Mindestanforderung zugelassen ist.

      Viele ältere OS-Versionen werden von BlackBerry UEM nicht mehr unterstützt. Sie müssen nur dann eine mindestens erforderliche Version auswählen, wenn Sie die früheste Version, die derzeit von BlackBerry UEM unterstützt wird, nicht zulassen möchten. Weitere Informationen zu den unterstützten Versionen finden Sie in der Kompatibilitätsmatrix.
   d) Wählen Sie die unterstützten Aktivierungstypen aus.

      Für Android-Geräte können Sie mehrere Aktivierungsarten auswählen und sie nach Rangordnung einstufen. Für alle anderen Gerätetypen können Sie nur eine Aktivierungsart auswählen.

      Die Aktivierungsart „MDM-Steuerelemente“ wird für Geräte mit Android 10 und höher nicht mehr unterstützt. Sie ist nur dann in der Liste der Aktivierungsarten enthalten, wenn die Einstellung **Aktivierungsart der MDM-Steuerelemente für Android-Geräte aktivieren** in den standardmäßigen Aktivierungseinstellungen ausgewählt ist.
10. Führen Sie für Android-Geräte die folgenden Aktionen durch:
    a) Wenn Sie mehr als eine Aktivierungsart ausgewählt haben, klicken Sie auf den Abwärts- bzw. Aufwärtspfeil, um die Rangfolge festzulegen.

       Geräte erhalten das von ihnen unterstützte Profil mit der höchsten Rangfolge. Wenn Sie beispielsweise „MDM-Steuerelemente“ den ersten Rang zuweisen, erhalten Geräte, die „MDM-Steuerelemente“ nicht unterstützen, den an nächster Stelle stehenden Aktivierungstyp.
    b) Wenn Sie die Aktivierungsart „MDM-Steuerelemente“ auswählen und nicht möchten, dass die Knox MDM-Richtlinienregeln auf die Geräte angewandt werden, die sie unterstützen, deaktivieren Sie das Kontrollkästchen **Samsung KNOX APIs auf den Aktivierungsarten 'MDM-Steuerelemente' aktivieren**.

c) Wenn Sie eine der Samsung Knox-Aktivierungsarten auswählen und Google Play für die Verwaltung von geschäftlichen Apps verwenden möchten, wählen Sie **Google Play-App-Verwaltung für Samsung Knox Workspace-Geräte**. Diese Option ist nur verfügbar, wenn Sie eine Verbindung zu einer Google-Domäne konfiguriert haben.

   Samsung Knox-Aktivierungsarten werden in einer zukünftigen Version nicht mehr unterstützt. Geräte, die Knox Platform for Enterprise unterstützen, können über die Android Enterprise-Aktivierungsarten aktiviert werden. Weitere Informationen finden Sie in Artikel 54614 unter https://support.blackberry.com/community.

d) Wenn Sie eine der Android Enterprise-Aktivierungsarten ausgewählt haben, aktivieren Sie die entsprechenden Android Enterprise-Optionen:

   Samsung

   - Die Option **Bei der Aktivierung von Android Enterprise-Geräten Premium UEM-Funktionen wie z. B. BlackBerry Secure Connect Plus freischalten** aktiviert BlackBerry Secure Connect Plus und die Knox-Plattform für Enterprise-Funktionen (für Geräte, die Samsung Knox unterstützen) auf Geräten mit einer entsprechenden Lizenz.
   - **Samsung Knox DualDAR Workspace aktivieren** aktiviert die Samsung Knox DualDAR-Verschlüsselung für Geräte, die diese unterstützen. Diese Option wird nur von Geräten mit den Aktivierungsarten „Nur geschäftlicher Bereich“ und „Geschäftlich und persönlich – volle Kontrolle“ unterstützt.
   - **Google Play-Konto zum geschäftlichen Bereich hinzufügen** ermöglicht die Verwaltung von Google Play-Apps im geschäftlichen Bereich. Wenn das Gerät keinen Zugriff auf Google Play hat, deaktivieren Sie diese Option.
   - **Nur genehmigte Geräte-IDs zulassen** ermöglicht es Ihnen, die Aktivierung auf einzelne Geräte zu beschränken, für die Sie die Geräte-ID angeben. Diese Option wird nur von Geräten mit den Aktivierungsarten „Nur geschäftlicher Bereich“ und „Geschäftlich und persönlich – volle Kontrolle“ unterstützt.

e) Wählen Sie im Abschnitt **Optionen für SafetyNet-Nachweis** optional eine der folgenden Nachweismethoden aus:

   - **SafetyNet-Nachweis für Gerät durchführen**: Verwenden Sie diese Methode, um Prüffragen zum Testen der Authentizität und Integrität der Geräte zu senden.
   - **SafetyNet-Nachweis bei Geräteaktivierung durchführen**: Verwenden Sie diese Methode, um Prüffragen zum Testen der Authentizität und Integrität der Geräte zu senden, wenn sie aktiviert werden.
   - **SafetyNet-Nachweis bei der Aktivierung der BlackBerry Dynamics-App durchführen**: Verwenden Sie diese Methode, um Prüffragen zum Testen der Authentizität und Integrität der BlackBerry Dynamics-Apps zu senden, wenn sie aktiviert werden.

f) Wählen Sie im Abschnitt **Optionen für Hardware-Nachweis** die Option **Konformitätsregeln für den Integritätsnachweis während der Aktivierung durchsetzen** aus, wenn BlackBerry UEM bei Aktivierung der Geräte Nachweise senden soll, um sicherzustellen, dass die erforderliche Sicherheits-Patch-Stufe installiert ist.

11. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Legen Sie ggf. eine Rangfolge für die Profile fest.

Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz

Die folgenden Schritte gelten nur für Geräte, denen die Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) zugewiesen ist. Geräte mit diese Aktivierungsart müssen vor der Aktivierung nicht auf die Werkseinstellungen zurückgesetzt werden.

Senden Sie die folgenden Aktivierungsanweisungen an die Gerätebenutzer, oder senden Sie ihnen einen Link zum folgenden Workflow: Aktivieren Ihres Android-Geräts.

Bevor Sie beginnen: Ihr Geräteadministrator hat Ihnen eine oder mehrere E-Mail-Nachrichten mit den Informationen gesendet, die Sie zur Aktivierung Ihres Geräts benötigen. Wenn die E-Mail einen QR Code für die Aktivierung enthält, können Sie diesen zum Aktivieren des Geräts verwenden und müssen keine weiteren Informationen eingeben. Wenn Sie keinen QR Code erhalten haben, vergewissern Sie sich, dass Sie die folgenden Informationen erhalten haben:

- Ihre geschäftliche E-Mail-Adresse
- BlackBerry UEM-Benutzername (in der Regel Ihr geschäftlicher Benutzername)
- BlackBerry UEM-Aktivierungskennwort
- BlackBerry UEM Serveradresse (falls erforderlich)

1. Installieren Sie den BlackBerry UEM Client von Google Play auf dem Gerät.

   Wenn das Gerät keinen Zugriff auf Google Play hat, können Sie den UEM Client manuell von BlackBerry herunterladen und installieren. Um die APK-Datei der neuesten UEM Client-App herunterzuladen, besuchen Sie support.blackberry.com/community, und lesen Sie Artikel 42607.
2. Öffnen Sie den UEM Client.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
4. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren Sie das Gerät mit einem QR Code.	**a.** Tippen Sie auf . **b.** Tippen Sie auf **Zulassen**, damit der UEM Client Fotos und Videos aufnehmen kann. **c.** Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.
Manuelles Aktivieren des Geräts	**a.** Geben Sie Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf **Weiter**. **b.** Geben Sie Ihr Aktivierungskennwort ein. Tippen Sie auf **Mein Gerät aktivieren**. **c.** Geben Sie ggf. die Serveradresse ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service. Tippen Sie auf **Weiter**. **d.** Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein. Tippen Sie auf **Weiter**.

5. Tippen Sie auf **Zulassen**, um UEM Client das Tätigen und Verwalten von Telefonanrufen zu gestatten.
6. Warten Sie, während die Profile und Einstellungen an Ihr Gerät übertragen werden.
7. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**, und warten Sie, bis ein geschäftliches Profil auf dem Gerät eingerichtet wurde.
8. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto mit Ihrer Google-E-Mail-Adresse und Ihrem Kennwort an.
9. Wählen Sie auf dem Bildschirm zur Auswahl der Entsperrmethode eine Entsperrmethode aus.
10. Wenn der Bildschirm **Sicheres Starten** angezeigt wird, tippen Sie auf **Ja**, damit zum Starten des Geräts ein Kennwort erforderlich ist.
11. Geben Sie ein Gerätekennwort ein, und wiederholen Sie es zur Bestätigung. Tippen Sie auf **OK**.
12. Wählen Sie eine der Optionen aus, um festzulegen, wie Ihre Benachrichtigungen angezeigt werden sollen. Tippen Sie auf **Fertig**.

13. Erstellen Sie ein UEM Client Kennwort, und tippen Sie auf **OK**. Wenn Sie BlackBerry Dynamics-Apps verwenden, verwenden Sie auch dieses Kennwort, um sich bei allen BlackBerry Dynamics-Apps anzumelden.
14. Tippen Sie auf dem nächsten Bildschirm auf **Anmelden**, und befolgen Sie die Anweisungen auf dem Bildschirm, wenn Sie die Authentifizierung per Fingerabdruck für den UEM Client und alle BlackBerry Dynamics-Apps einrichten möchten. Tippen Sie andernfalls auf **Abbrechen**.
15. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die BlackBerry UEM-Aktivierung abzuschließen.
16. Wenn Sie dazu aufgefordert werden, tippen Sie auf **OK**, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
17. Wenn Sie dazu aufgefordert werden, folgen Sie den Anweisungen auf dem Bildschirm, um geschäftliche Apps auf Ihrem Gerät zu installieren.

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

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

Aktivieren eines Android Enterprise-Geräts, wenn BlackBerry UEM mit einer Google-Domäne verbunden ist

Diese Schritte gelten für Geräte, denen die Aktivierungsart Nur geschäftlicher Bereich (Android Enterprise) oder Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) zugewiesen ist, wenn BlackBerry UEM mit einer G Suite- oder Google Cloud-Domäne verbunden ist. Informationen zum Aktivieren von Geräten, die mit einer Google-Domäne mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz verbunden sind, finden Sie unter Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz.

In diesem Thema wird eine Methode zum Aktivieren von Android Enterprise-Geräten beschrieben. Informationen zu weiteren Optionen finden Sie unter Aktivieren von Android-Geräten.

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

Bevor Sie beginnen: Ihr Geräteadministrator hat Ihnen eine oder mehrere E-Mail-Nachrichten mit den Informationen gesendet, die Sie zur Aktivierung Ihres Geräts benötigen. Wenn die E-Mail einen QR Code für die Aktivierung enthält, können Sie diesen zum Aktivieren des Geräts verwenden und müssen keine weiteren Informationen eingeben. Wenn Sie keinen QR Code erhalten haben, vergewissern Sie sich, dass Sie die folgenden Informationen erhalten haben:

- Ihre geschäftliche E-Mail-Adresse
- BlackBerry UEM Aktivierungsbenutzername (in der Regel Ihr geschäftlicher Benutzername)
- BlackBerry UEM-Aktivierungskennwort
- BlackBerry UEM Serveradresse (falls erforderlich)

1. Wenn Ihnen der Willkommen-Bildschirm der Geräteeinrichtung nicht angezeigt wird, setzen Sie das Gerät auf die werksseitigen Standardeinstellungen zurück.
2. Geben Sie während der Einrichtung des Geräts auf dem Anmeldebildschirm des Google-Kontos Ihre geschäftliche Google-E-Mail-Adresse und Ihr Kennwort ein.
3. Tippen Sie auf dem Gerät auf **Installieren**, um den BlackBerry UEM Client zu installieren.

4. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
5. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren Sie das Gerät mit einem QR Code.	**a.** Tippen Sie auf . **b.** Tippen Sie auf **Zulassen**, damit der UEM Client Fotos und Videos aufnehmen kann. **c.** Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.
Manuelles Aktivieren des Geräts	**a.** Geben Sie Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf **Weiter**. **b.** Geben Sie Ihr Aktivierungskennwort ein. Tippen Sie auf **Mein Gerät aktivieren**. **c.** Geben Sie ggf. die Serveradresse ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service. Tippen Sie auf **Weiter**. **d.** Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein. Tippen Sie auf **Weiter**.

6. Warten Sie, während die Profile und Einstellungen an Ihr Gerät übertragen werden.
7. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**, und warten Sie, bis ein geschäftliches Profil auf dem Gerät eingerichtet wurde.
8. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto mit Ihrer Google-E-Mail-Adresse und Ihrem Kennwort an.
9. Wählen Sie auf dem Bildschirm zur Auswahl der Entsperrmethode eine Entsperrmethode aus.
10. Wenn der Bildschirm **Sicheres Starten** angezeigt wird, tippen Sie auf **Ja**, damit zum Starten des Geräts ein Kennwort erforderlich ist.
11. Geben Sie ein Gerätekennwort ein, und wiederholen Sie es zur Bestätigung. Tippen Sie auf **OK**.
12. Wählen Sie eine der Optionen aus, um festzulegen, wie Ihre Benachrichtigungen angezeigt werden sollen. Tippen Sie auf **Fertig**.
13. Erstellen Sie ein UEM Client Kennwort, und tippen Sie auf **OK**. Wenn Sie BlackBerry Dynamics-Apps verwenden, verwenden Sie auch dieses Kennwort, um sich bei allen BlackBerry Dynamics-Apps anzumelden.
14. Tippen Sie auf dem nächsten Bildschirm auf **Anmelden**, und befolgen Sie die Anweisungen auf dem Bildschirm, wenn Sie die Authentifizierung per Fingerabdruck für den UEM Client und alle BlackBerry Dynamics-Apps einrichten möchten. Tippen Sie andernfalls auf **Abbrechen**.
15. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die BlackBerry UEM-Aktivierung abzuschließen.
16. Wenn Sie dazu aufgefordert werden, tippen Sie auf **OK**, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
17. Wenn Sie dazu aufgefordert werden, folgen Sie den Anweisungen auf dem Bildschirm, um geschäftliche Apps auf Ihrem Gerät zu installieren.

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

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

Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Nur geschäftlicher Bereich mithilfe eines verwalteten Google Play-Kontos

In diesem Thema wird eine Methode zum Aktivieren von Android Enterprise-Geräten beschrieben. Informationen zu weiteren Optionen finden Sie unter Aktivieren von Android-Geräten.

Diese Anweisungen gelten auch für Android 10-Geräte mit der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle.

Für Android-Geräte mit den Versionen 8 und 9 finden Sie Informationen unter Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle mithilfe eines verwalteten Google Play-Kontos. Auf Android-Geräten mit den Versionen 8 und 9 wird die Verwendung des afw#BlackBerry-Hashtags zum Starten von Nur geschäftlicher Bereich- oder Geschäftlich und persönlich – vollständige Kontrolle-Aktivierungen nicht mehr unterstützt.

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

Bevor Sie beginnen: Ihr Geräteadministrator hat Ihnen eine oder mehrere E-Mail-Nachrichten mit den Informationen gesendet, die Sie zur Aktivierung Ihres Geräts benötigen. Wenn Sie von Ihrem Administrator einen QR Code für die Aktivierung erhalten haben, können Sie diesen zum Aktivieren Ihres Geräts verwenden und müssen keine weiteren Informationen eingeben. Wenn Sie keinen QR Code erhalten haben, vergewissern Sie sich, dass Sie die folgenden Informationen erhalten haben:

- Ihre geschäftliche E-Mail-Adresse
- BlackBerry UEM Aktivierungsbenutzername (in der Regel Ihr geschäftlicher Benutzername)
- BlackBerry UEM-Aktivierungskennwort
- BlackBerry UEM Serveradresse (falls erforderlich)

1. Wenn Ihnen der Willkommen-Bildschirm der Geräteeinrichtung nicht angezeigt wird, setzen Sie das Gerät auf die werksseitigen Standardeinstellungen zurück.
2. Geben Sie während der Einrichtung des Geräts afw#blackberry auf dem Anmeldebildschirm des Google-Kontos ein.
3. Tippen Sie auf **Installieren**, um BlackBerry UEM Client zu installieren.
4. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
5. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren Sie das Gerät mit einem QR Code.	**a.** Tippen Sie auf . **b.** Tippen Sie auf **Zulassen**, damit der UEM Client Fotos und Videos aufnehmen kann. **c.** Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.
Manuelles Aktivieren des Geräts	**a.** Geben Sie Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf **Weiter**. **b.** Geben Sie Ihr Aktivierungskennwort ein. Tippen Sie auf **Mein Gerät aktivieren**. **c.** Geben Sie ggf. die Serveradresse ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service. Tippen Sie auf **Weiter**.

Aufgabe	Schritte
	d. Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein. Tippen Sie auf **Weiter**.

6. Warten Sie, während die Profile und Einstellungen an Ihr Gerät übertragen werden.
7. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**, und warten Sie, bis ein geschäftliches Profil auf dem Gerät eingerichtet wurde.
8. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto mit Ihrer Google-E-Mail-Adresse und Ihrem Kennwort an.
9. Wählen Sie auf dem Bildschirm zur Auswahl der Entsperrmethode eine Entsperrmethode aus.
10. Wenn der Bildschirm **Sicheres Starten** angezeigt wird, tippen Sie auf **Ja**, damit zum Starten des Geräts ein Kennwort erforderlich ist.
11. Geben Sie ein Gerätekennwort ein, und wiederholen Sie es zur Bestätigung. Tippen Sie auf **OK**.
12. Wählen Sie eine der Optionen aus, um festzulegen, wie Ihre Benachrichtigungen angezeigt werden sollen. Tippen Sie auf **Fertig**.
13. Erstellen Sie ein UEM Client Kennwort, und tippen Sie auf **OK**. Wenn Sie BlackBerry Dynamics-Apps verwenden, verwenden Sie auch dieses Kennwort, um sich bei allen BlackBerry Dynamics-Apps anzumelden.
14. Tippen Sie auf dem nächsten Bildschirm auf **Anmelden**, und befolgen Sie die Anweisungen auf dem Bildschirm, wenn Sie die Authentifizierung per Fingerabdruck für den UEM Client und alle BlackBerry Dynamics-Apps einrichten möchten. Tippen Sie andernfalls auf **Abbrechen**.
15. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die BlackBerry UEM-Aktivierung abzuschließen.
16. Wenn Sie dazu aufgefordert werden, tippen Sie auf **OK**, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
17. Wenn Sie dazu aufgefordert werden, folgen Sie den Anweisungen auf dem Bildschirm, um geschäftliche Apps auf Ihrem Gerät zu installieren.

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

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

Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle mithilfe eines verwalteten Google Play-Kontos

In diesem Thema wird eine Methode zum Aktivieren von Android Enterprise-Geräten beschrieben. Informationen zu weiteren Optionen finden Sie unter Aktivieren von Android-Geräten.

Bei Android 10-Geräten funktionieren die Anweisungen zum Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Nur geschäftlicher Bereich mithilfe eines verwalteten Google Play-Kontos auch für die Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle. Ab Android 11 wird die Verwendung des Hashtags afw#BlackBerry zum Initiieren von Geschäftlich und persönlich – vollständige Kontrolle-Aktivierungen nicht mehr unterstützt.

Diese Anweisungen beinhalten die Verwendung eines QR Code s mit Anweisungen zum Herunterladen und Installieren des BlackBerry UEM Client s. Damit Benutzer den Download mit dem QR Code durchführen können, müssen Sie in den standardmäßigen Aktivierungseinstellungen **Zulassen, dass der QR-Code den Speicherort der Quelldatei der UEM-Client-App enthält** auswählen. Weitere Informationen finden Sie unter Festlegen der standardmäßigen Aktivierungseinstellungen.

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

Bevor Sie beginnen: Ihr Geräteadministrator hat Ihnen eine oder mehrere E-Mail-Nachrichten mit den Informationen gesendet, die Sie zur Aktivierung Ihres Geräts benötigen. Die E-Mail-Nachricht enthält einen QR Code mit den Informationen, die zum Installieren von UEM Client und zum Aktivieren des Geräts erforderlich sind.

1. Wenn Ihnen auf dem zu aktivierenden Gerät der Bildschirm für die Geräteeinrichtung nicht angezeigt wird, setzen Sie das Gerät auf die werksseitigen Standardeinstellungen zurück.
2. Tippen Sie siebenmal auf den Gerätebildschirm.

   Auf dem Gerät wird ein QR Code-Leser geöffnet.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
4. Warten Sie, während die Profile und Einstellungen an Ihr Gerät übertragen werden.
5. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**, und warten Sie, bis ein geschäftliches Profil auf dem Gerät eingerichtet wurde.
6. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto mit Ihrer Google-E-Mail-Adresse und Ihrem Kennwort an.
7. Wählen Sie auf dem Bildschirm zur Auswahl der Entsperrmethode eine Entsperrmethode aus.
8. Wenn der Bildschirm **Sicheres Starten** angezeigt wird, tippen Sie auf **Ja**, damit zum Starten des Geräts ein Kennwort erforderlich ist.
9. Geben Sie ein Gerätekennwort ein, und wiederholen Sie es zur Bestätigung. Tippen Sie auf **OK**.
10. Wählen Sie eine der Optionen aus, um festzulegen, wie Ihre Benachrichtigungen angezeigt werden sollen. Tippen Sie auf **Fertig**.
11. Erstellen Sie ein UEM Client Kennwort, und tippen Sie auf **OK**. Wenn Sie BlackBerry Dynamics-Apps verwenden, verwenden Sie auch dieses Kennwort, um sich bei allen BlackBerry Dynamics-Apps anzumelden.
12. Tippen Sie auf dem nächsten Bildschirm auf **Anmelden**, und befolgen Sie die Anweisungen auf dem Bildschirm, wenn Sie die Authentifizierung per Fingerabdruck für den UEM Client und alle BlackBerry Dynamics-Apps einrichten möchten. Tippen Sie andernfalls auf **Abbrechen**.
13. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die BlackBerry UEM-Aktivierung abzuschließen.
14. Wenn Sie dazu aufgefordert werden, tippen Sie auf **OK**, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
15. Wenn Sie dazu aufgefordert werden, folgen Sie den Anweisungen auf dem Bildschirm, um geschäftliche Apps auf Ihrem Gerät zu installieren.

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

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

Aktivieren eines Android Enterprise-Geräts ohne Zugriff auf Google Play

Diese Schritte gelten für die Aktivierung von Android-Geräten ohne Zugriff auf Google Play mit den Aktivierungsarten Nur geschäftlicher Bereich (Android Enterprise) und Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise). Informationen zum Aktivieren von Geräten mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) finden Sie unter: Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz.

Um mit der Aktivierung zu beginnen, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden, und die Anweisungen zum Herunterladen von BlackBerry UEM Client mit einem QR Code oder NFC müssen vorliegen.

- Sie können den Download-Speicherort für den UEM Client in den QR-Code, den Benutzer in der Aktivierungs-E-Mail erhalten, aufnehmen. Benutzer können den QR Code scannen, um den Download zu starten. Weitere Informationen finden Sie unter Standardmäßige Geräteaktivierungseinstellungen.
- Sie können einen NFC-Sticker vorprogrammieren, den Benutzer antippen können, um die Geräteaktivierung zu starten.
- Bei Android-Geräten bis Version 9 können Benutzer NFC verwenden und auf ein zweites Gerät tippen, auf dem die BlackBerry UEM Enroll-App installiert ist. Um die UEM Enroll-App auf ein sekundäres Gerät herunterzuladen und zu installieren, lesen Sie Artikel 42607 unter support.blackberry.com/community.

Über das gleiche sekundäre Gerät oder den NFC-Sticker können Geräte für mehrere Benutzer aktiviert werden.

Wenn Sie möchten, dass der Benutzer die Geräteaktivierung mit einem QR Code initiiert, senden Sie die Aktivierungsanweisungen für Aktivieren eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle mithilfe eines verwalteten Google Play-Kontos an den Gerätebenutzer.

Wenn Sie möchten, dass der Benutzer die Geräteaktivierung über NFC initiiert, senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer:

Bevor Sie beginnen:

- Ihr Geräteadministrator hat Ihnen eine oder mehrere E-Mail-Nachrichten mit den Informationen gesendet, die Sie zur Aktivierung Ihres Geräts benötigen. Wenn Sie von Ihrem Administrator einen QR Code für die Aktivierung erhalten haben, können Sie diesen zum Aktivieren Ihres Geräts verwenden und müssen keine weiteren Informationen eingeben. Wenn Sie keinen QR Code erhalten haben, vergewissern Sie sich, dass Sie die folgenden Informationen erhalten haben:
  - Ihre geschäftliche E-Mail-Adresse
  - BlackBerry UEM Aktivierungsbenutzername (in der Regel Ihr geschäftlicher Benutzername)
  - BlackBerry UEM-Aktivierungskennwort
  - BlackBerry UEM Serveradresse (falls erforderlich)
- Ihr Administrator stellt Ihnen einen vorprogrammierten NFC-Sticker oder ein sekundäres Gerät zur Verfügung, auf dem die UEM Enroll-App installiert ist.

1. Wenn Ihnen auf dem zu aktivierenden Gerät der Willkommen-Bildschirm der Geräteeinrichtung nicht angezeigt wird, setzen Sie das Gerät auf die werksseitigen Standardeinstellungen zurück.
2. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Starten der Aktivierung mit einem NFC-Sticker	**a.** Tippen Sie auf das Gerät mit dem NFC-Sticker, das Sie von Ihrem Administrator erhalten haben. Das Gerät lädt UEM Client herunter und installiert es.

Aufgabe	Schritte
	b. Folgen Sie der Aufforderung, während sich das Gerät auf die Aktivierung vorbereitet.
Initiieren der Aktivierung mit einem sekundären Gerät	**a.** Installieren Sie die UEM Enroll-App auf dem sekundären Gerät. Stellen Sie sicher, dass NFC auf dem Gerät aktiviert ist. **b.** Tippen Sie auf **Gerät aktivieren**. **c.** Halten Sie beide Geräte mit der Rückseite aneinander. Wenn Sie dazu aufgefordert werden, tippen Sie auf eine beliebige Stelle auf dem Bildschirm des sekundären Geräts. **d.** Befolgen Sie die Anweisungen auf dem Bildschirm des zu aktivierenden Geräts, um UEM Client herunterzuladen und zu installieren.

3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
4. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren Sie das Gerät mit einem QR Code.	**a.** Tippen Sie auf . **b.** Tippen Sie auf **Zulassen**, damit der UEM Client Fotos und Videos aufnehmen kann. **c.** Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.
Manuelles Aktivieren des Geräts	**a.** Geben Sie Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf **Weiter**. **b.** Geben Sie Ihr Aktivierungskennwort ein. Tippen Sie auf **Mein Gerät aktivieren**. **c.** Geben Sie ggf. die Serveradresse ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service. Tippen Sie auf **Weiter**. **d.** Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein. Tippen Sie auf **Weiter**.

5. Warten Sie, während die Profile und Einstellungen an Ihr Gerät übertragen werden.
6. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**, und warten Sie, bis ein geschäftliches Profil auf dem Gerät eingerichtet wurde.
7. Wählen Sie auf dem Bildschirm zur Auswahl der Entsperrmethode eine Entsperrmethode aus.
8. Wenn der Bildschirm **Sicheres Starten** angezeigt wird, tippen Sie auf **Ja**, damit zum Starten des Geräts ein Kennwort erforderlich ist.
9. Geben Sie ein Gerätekennwort ein, und wiederholen Sie es zur Bestätigung. Tippen Sie auf **OK**.
10. Wählen Sie eine der Optionen aus, um festzulegen, wie Ihre Benachrichtigungen angezeigt werden sollen. Tippen Sie auf **Fertig**.
11. Erstellen Sie ein UEM Client Kennwort, und tippen Sie auf **OK**. Wenn Sie BlackBerry Dynamics-Apps verwenden, verwenden Sie auch dieses Kennwort, um sich bei allen BlackBerry Dynamics-Apps anzumelden.
12. Tippen Sie auf dem nächsten Bildschirm auf **Anmelden**, und befolgen Sie die Anweisungen auf dem Bildschirm, wenn Sie die Authentifizierung per Fingerabdruck für den UEM Client und alle BlackBerry Dynamics-Apps einrichten möchten. Tippen Sie andernfalls auf **Abbrechen**.
13. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die BlackBerry UEM-Aktivierung abzuschließen.

14. Wenn Sie dazu aufgefordert werden, tippen Sie auf **OK**, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
15. Wenn Sie dazu aufgefordert werden, folgen Sie den Anweisungen auf dem Bildschirm, um geschäftliche Apps auf Ihrem Gerät zu installieren.
16. Öffnen Sie ggf. die E-Mail-App, die Ihr Unternehmen verwenden möchte, und befolgen Sie die Anweisungen zum Einrichten von E-Mails auf Ihrem Telefon.

Aktivierung eines Android-Geräts mit der Aktivierungsart MDM-Steuerelemente

Hinweis: Die folgenden Schritte gelten nur für Geräte, denen die Aktivierungsart MDM-Steuerelemente zugewiesen ist. Diese Aktivierungsart wird für Android 10 nicht 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.

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Installieren Sie den BlackBerry UEM Client von Google Play auf dem Gerät.
2. Öffnen Sie den UEM Client.
3. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
4. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren Sie das Gerät mit einem QR Code.	a. Tippen Sie auf . b. Tippen Sie auf **Zulassen**, damit der UEM Client Fotos und Videos aufnehmen kann. c. Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.
Manuelles Aktivieren des Geräts	a. Geben Sie Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf **Weiter**. b. Geben Sie Ihr Aktivierungskennwort ein. Tippen Sie auf **Mein Gerät aktivieren**. c. Geben Sie ggf. die Serveradresse ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service. Tippen Sie auf **Weiter**. d. Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein. Tippen Sie auf **Weiter**.

5. Tippen Sie auf **Weiter**.
6. Tippen Sie auf **Aktivieren**, um den Geräteadministrator zu aktivieren. Damit Sie auf geschäftliche Daten auf Ihrem Gerät zugreifen können, müssen Sie den Geräteadministrator aktivieren.
7. Wenn Sie dazu aufgefordert werden, tippen Sie auf **OK**, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
8. Wenn Sie dazu aufgefordert werden, folgen Sie den Anweisungen auf dem Bildschirm, um geschäftliche Apps auf Ihrem Gerät zu installieren.

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

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

Aktivierte Android-Geräte verwalten und überwachen

Wenn Geräte durch eine IT-Richtlinie und Profile aktiviert und verwaltet wurden, stehen Ihnen mehrere Funktionen zur Steuerung der Geräte der Benutzer zur Verfügung.

Sie haben folgende Wahlmöglichkeiten:

Option	Beschreibung
Steuern, welche Softwareupdates zu welchem Zeitpunkt auf den Geräten installiert werden	Auf folgenden Geräten können Sie über ein Profil für Gerätedienstanforderungen angeben, ob und wann das Betriebssystem aktualisiert werden soll: • Android Enterprise-Geräte mit einer Nur geschäftlicher Bereich-Aktivierung • Samsung Knox-Geräte Weitere Informationen finden Sie in der Dokumentation für Administratoren. In Kompatibilitätsprofilen können Sie angeben, ob Betriebssystemversionen gesperrt werden sollen. Weitere Informationen finden Sie in der Dokumentation für Administratoren.
Aktivieren der Standorteinstellungen und Ortung eines Geräts	Sie können Standorteinstellungen aktivieren, um Android-Geräte zu orten. Weitere Informationen finden Sie in der Dokumentation für Administratoren.
Geräteprotokolle auslesen	Sie können zu Überwachungs- und Fehlerbehebungszwecken Protokolle von Geräten abrufen. Weitere Informationen finden Sie in der Dokumentation für Administratoren.
Gerät deaktivieren	Wird ein Gerät durch Sie oder einen Benutzer deaktiviert, so wird die Verbindung zwischen dem Gerät und dem Benutzerkonto in BlackBerry UEM entfernt. Sie können das Gerät nicht verwalten, und das Gerät wird nicht mehr in der Verwaltungskonsole angezeigt. Der Benutzer kann nicht auf die geschäftlichen Daten auf dem Gerät zugreifen. Sie können ein Gerät mit dem Befehl „Alle Gerätedaten löschen“ oder „Nur Geschäftsdaten löschen“ deaktivieren. Benutzer können ein Android-Gerät deaktivieren, indem sie auf dem Bildschirm „Info“ in der BlackBerry UEM Client-App „Mein Gerät deaktivieren“ auswählen.

Befehle für Android-Geräte

Befehl	Beschreibung	Aktivierungsarten
Anzeigen des Geräteberichts	Durch diesen Befehl werden Detailinformationen zu einem Gerät angezeigt. Sie können den Gerätebericht exportieren und auf Ihrem Computer speichern. Weitere Informationen finden Sie unter Anzeigen und Speichern eines Geräteberichts.	Alle (außer BlackBerry 2FA)
Anzeigen der Geräteaktionen	Mit diesem Befehl werden alle Aktionen angezeigt, die gerade auf einem Gerät durchgeführt werden. Weitere Informationen finden Sie unter Anzeigen der Geräteaktionen.	Alle (außer BlackBerry 2FA)
Gerät sperren	Mit diesem Befehl sperren Sie das Gerät. Der Benutzer muss das bestehende Gerätekennwort eingeben, um das Gerät zu entsperren. Wenn ein Gerät vorübergehend verlegt wurde, können Sie diesen Befehl verwenden. Wenn Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt.	MDM-Steuerelemente Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Nur geschäftlicher Bereich (Android Enterprise)
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind, einschließlich der im geschäftlichen Bereich, und das Gerät wird auf die Werkseinstellungen zurückgesetzt. Wenn das Gerät keine Verbindung zu BlackBerry UEM herstellen kann, wenn Sie diesen Befehl senden, können Sie den Befehl entweder abbrechen oder das Gerät aus der Konsole entfernen. Wenn das Gerät eine Verbindung zu BlackBerry UEM herstellt, nachdem es entfernt wurde, werden nur die Geschäftsdaten vom Gerät gelöscht. Falls zutreffend, wird auch der geschäftliche Bereich entfernt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)

Befehl	Beschreibung	Aktivierungsarten
Nur geschäftliche Daten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht, und das Gerät wird deaktiviert. Wenn das Gerät über einen geschäftlichen Bereich verfügt, werden die Informationen im geschäftlichen Bereich sowie der Bereich selbst vom Gerät gelöscht, aber alle persönlichen Apps und Daten verbleiben auf dem Gerät. Weitere Informationen finden Sie unter Deaktivieren von Geräten. Wenn Sie diesen Befehl auf Android Enterprise-Geräten verwenden, können Sie einen Grund für das Löschen des geschäftlichen Profils eingeben, der in der Benachrichtigung auf dem Gerät des Benutzers angezeigt wird. Bei den Aktivierungsarten Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) wird dieser Befehl nur von Geräten mit Android 11 und höher unterstützt. Wenn das Gerät keine Verbindung zu BlackBerry UEM herstellen kann, wenn Sie diesen Befehl senden, können Sie den Befehl entweder abbrechen oder das Gerät aus der Konsole entfernen. Wenn das Gerät eine Verbindung zu BlackBerry UEM herstellt, nachdem es gelöscht wurde, werden die Geschäftsdaten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)
Gerät entsperren und Kennwort löschen	Mit diesem Befehl wird das Gerät gesperrt und der Benutzer zum Erstellen eines neuen Gerätekennworts aufgefordert. Wenn der Benutzer den Bildschirm „Gerätekennwort erstellen“ überspringt, wird das vorherige Kennwort beibehalten. Sie können diesen Befehl verwenden, wenn ein Benutzer sein Gerätekennwort vergessen hat. **Hinweis:** Dieser Befehl wird auf Geräten mit Samsung Knox SDK 3.2.1 oder höher nicht unterstützt.	MDM-Steuerelemente (nur Samsung-Geräte) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)

Befehl	Beschreibung	Aktivierungsarten
Gerätekennwort festlegen und sperren	Mit diesem Befehl können Sie ein Gerätekennwort erstellen und das Gerät anschließend sperren. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Um das Gerät zu entsperren, muss der Benutzer das neue Kennwort eingeben. **Hinweis:** Für die Aktivierungsarten Geschäftlich und persönlich – Benutzer-Datenschutz unterstützen nur BlackBerry-Geräte mit Android 8.x und höher diesen Befehl. **Hinweis:** Bei der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) wird dieser Befehl nur von Geräten mit einer Android OS-Version unterstützt, die älter als Android 11 ist.	Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Nur geschäftlicher Bereich (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)
Kennwort für geschäftlichen Bereich zurücksetzen	Dieser Befehl löscht das aktuelle Kennwort für den geschäftlichen Bereich vom Gerät. Wenn der Benutzer den geschäftlichen Bereich öffnet, fordert das Gerät ihn auf, ein neues Kennwort für den geschäftlichen Bereich festzulegen.	Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz - (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)
Geschäftlichen Bereich sperren und Kennwort festlegen	Sie können ein Kennwort für das geschäftliche Profil angeben und das Gerät sperren. Wenn der Benutzer eine geschäftliche App öffnet, muss er das von Ihnen festgelegte Kennwort eingeben.	Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)
Geschäftlichen Bereich aktivieren/ deaktivieren	Dieser Befehl aktiviert bzw. deaktiviert den Zugriff auf die Apps für den geschäftlichen Bereich auf dem Gerät.	Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz - (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)
BlackBerry 2FA deaktivieren	Mit diesem Befehl werden Geräte deaktiviert, die mit der Aktivierungsart BlackBerry 2FA aktiviert wurden. Das Gerät wird von BlackBerry UEM entfernt, und der Benutzer kann die Funktion BlackBerry 2FA nicht mehr verwenden.	BlackBerry 2FA

Befehl	Beschreibung	Aktivierungsarten
Apps bereinigen	Mit diesem Befehl werden die Daten von allen mit Microsoft Intune verwalteten Apps auf dem Gerät bereinigt. Die Apps werden nicht vom Gerät entfernt. Weitere Informationen finden Sie unter Von Microsoft Intune verwaltete Apps löschen.	Alle (außer BlackBerry 2FA)
Gerätedaten aktualisieren	Dieser Befehl sendet und empfängt aktualisierte Gerätedaten. Beispielsweise können Sie kürzlich aktualisierte IT-Richtlinienregeln oder Profile an ein Gerät senden und aktualisierte Informationen zu einem Gerät, wie Betriebssystemversion oder Akkuladezustand, empfangen. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	Alle (außer BlackBerry 2FA)
Fehlerbericht anfordern	Dieser Befehl fordert Client-Protokolle vom Gerät an. Der Gerätebenutzer muss die Anfrage annehmen oder ablehnen.	Nur geschäftlicher Bereich (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)
Gerät neu starten	Dieser Befehl sendet eine Neustart-Anforderung an das Gerät. Dem Benutzer wird eine Meldung angezeigt, dass das Gerät in einer Minute neu gestartet wird. Der Gerätebenutzer kann den Neustart 10 Minuten lang verzögern.	Nur geschäftlicher Bereich (Android Enterprise)
Gerät entfernen	Dieser Befehl entfernt das Gerät aus BlackBerry UEM, entfernt aber keine Daten vom Gerät. Das Gerät empfängt ggf. weiterhin E-Mails und andere geschäftliche Daten. Dieser Befehl ist für Geräte vorgesehen, die unwiederbringlich verloren gegangen sind oder beschädigt wurden und erwartungsgemäß keine erneute Verbindung zum Server herstellen werden. Wenn ein Gerät, das entfernt wurde, BlackBerry UEM zu kontaktieren versucht, erhält der Benutzer eine Benachrichtigung. Das Gerät kann erst dann wieder mit BlackBerry UEM kommunizieren, wenn es erneut aktiviert wurde. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	Alle (außer BlackBerry 2FA)

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