



# **BlackBerry UEM**

## **Aktivieren von Geräten**

12.20



# Contents

<b>Aktivieren von Geräten mit BlackBerry UEM.....</b>	<b>5</b>
Aktivierungsarten: iOS-Geräte.....	6
Aktivierungsarten: Android-Geräte.....	8
Aktivierungsarten: macOS-Geräte.....	13
Aktivierungsarten: Windows 10-Geräte.....	13
<b>Verwalten von Aktivierungseinstellungen.....</b>	<b>14</b>
Konfigurieren der standardmäßigen Aktivierungseinstellungen.....	14
Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail-Nachricht.....	14
Senden einer Aktivierungs-E-Mail an mehrere Benutzer.....	15
Zulassen, dass Benutzer Aktivierungskennwörter festlegen in BlackBerry UEM Self-Service.....	16
Aktivierung mehrerer Geräte mit verschiedenen Aktivierungsarten durch Benutzer zulassen.....	16
Erzwingen des Ablaufens von Aktivierungskennwörtern.....	17
<b>Unterstützung von Android Enterprise- und Android Management-Aktivierungen.....</b>	<b>18</b>
Unterstützung von Android Enterprise- und Android Management-Aktivierungen mithilfe verwalteter Google Play-Konten.....	18
Unterstützen von Android Enterprise-Aktivierungen mit einer Google Workspace-Domäne.....	18
Unterstützen von Android Enterprise-Aktivierungen mit einer Google Cloud-Domäne.....	19
Unterstützung von Android Enterprise-Geräten ohne Zugriff auf Google Play.....	19
<b>Unterstützen von Windows 10-Aktivierungen.....</b>	<b>22</b>
<b>Unterstützung der Apple-Benutzerregistrierung auf iOS- und iPadOS-Geräten.....</b>	<b>23</b>
<b>Unterstützung von Samsung Knox DualDAR.....</b>	<b>24</b>
<b>Erstellen von Aktivierungsprofilen.....</b>	<b>25</b>
Erstellen eines Aktivierungsprofils.....	25
<b>Aktivieren von Android-Geräten.....</b>	<b>28</b>
Aktivierung eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz.....	30
Aktivieren eines Android Enterprise-Geräts, wenn BlackBerry UEM mit einer Google-Domäne verbunden ist.....	32
Aktivieren eines Android Enterprise-Geräts mit einem verwalteten Google Play-Konto.....	33

Aktivieren eines Android Enterprise-Geräts ohne Zugriff auf Google Play.....	34
Aktivieren eines Android Management-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz.....	36
Aktivieren eines Android Management-Geräts mit einem verwalteten Google Play-Konto.....	37
<b>Aktivieren von iOS-Geräten.....</b>	<b>39</b>
Aktivierung eines iOS- oder iPadOS-Geräts mit der Aktivierungsart MDM-Steuerelemente.....	39
Aktivieren eines iOS- oder iPadOS-Geräts mit Apple-Benutzerregistrierung.....	40
<b>Aktivieren eines macOS- oder Apple TV-Geräts mit BlackBerry UEM Self- Service.....</b>	<b>42</b>
<b>Aktivieren eines Windows 10-Tablets oder -Computers.....</b>	<b>43</b>
<b>Konfigurieren der Unterstützung für die Android Zero-Touch-Registrierung....</b>	<b>45</b>
<b>Aktivieren von mehreren Geräten mit Knox Mobile Enrollment.....</b>	<b>46</b>
<b>Aktivieren von beim DEP registrierten iOS-Geräten.....</b>	<b>47</b>
Registrieren von iOS-Geräten in DEP und Zuweisen eines BlackBerry UEM-Servers.....	48
DEP-Registrierungskonfiguration hinzuzufügen.....	48
Einem iOS-Gerät einen Benutzer zuweisen.....	50
<b>Aktivieren von iOS-Geräten mit Apple Configurator 2.....</b>	<b>52</b>
Hinzufügen von BlackBerry UEM-Serverinformationen zu Apple Configurator 2.....	52
Vorbereiten von iOS-Geräten mit Apple Configurator 2.....	53
<b>Importieren oder exportieren einer Liste genehmigter Geräte-IDs.....</b>	<b>54</b>
<b>Deaktivieren von Geräten.....</b>	<b>55</b>
<b>Fehlerbehebung der Geräteaktivierung.....</b>	<b>56</b>
Fehlerbehebung: Aktivierungsfehler und -probleme.....	57
<b>Rechtliche Hinweise.....</b>	<b>59</b>

# Aktivieren von Geräten mit BlackBerry UEM

Wenn Sie oder ein Benutzer ein Gerät aktivieren, ist das Gerät mit BlackBerry UEM verknüpft. Dies ermöglicht Ihnen die Verwaltung und Zuweisung von Konfigurationen zu Geräten und gibt Benutzern Zugriff auf geschäftliche Daten auf ihren Geräten.

Wenn ein Gerät aktiviert wurde, können Sie IT-Richtlinien und Profile versenden, um Funktionen zu überwachen und konfigurieren und die Sicherheit der geschäftlichen Daten sicherzustellen. Sie können auch Apps zuweisen, die der Benutzer installieren kann. Je nachdem, wie viel Kontrolle die ausgewählte Aktivierungsart zulässt, können Sie das Gerät auch dadurch schützen, dass Sie den Zugriff auf bestimmte Daten einschränken, dezentral Kennwörter festlegen, das Gerät sperren oder Daten löschen.

Sie können die Aktivierungsarten so zuweisen, dass die besonderen Anforderungen individuell umgesetzt werden, je nachdem, ob die Geräte Ihrem Unternehmen oder den Benutzern gehören. Durch die verschiedenen Aktivierungsarten haben Sie einen unterschiedlich hohen Einfluss auf die geschäftlichen und privaten Daten auf den Geräten: von der kompletten Kontrolle aller Daten bis hin zur Beschränkung der Kontrolle auf die geschäftlichen Daten.

Um UEM so einzurichten, dass Benutzer Geräte aktivieren können, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Überprüfen Sie für jedes Gerät, das Sie aktivieren möchten, ob eine UEM-Lizenz verfügbar ist. Überprüfen Sie bei iOS-, iPadOS- und Android-Geräten, ob die neueste Version von BlackBerry UEM Client im entsprechenden App Store auf dem Gerät installiert ist.
2	Konfigurieren der standardmäßigen Aktivierungseinstellungen.
3	Überprüfen Sie die Informationen, die für Ihre UEM-Umgebung und Gerätebenutzer relevant sind: <ul style="list-style-type: none"><li>• Unterstützung von Android Enterprise- und Android Management-Aktivierungen</li><li>• Unterstützen von Windows 10-Aktivierungen</li><li>• Unterstützung der Apple-Benutzerregistrierung auf iOS- und iPadOS-Geräten</li><li>• Unterstützung von Samsung Knox DualDAR</li><li>• Konfigurieren der Unterstützung für die Android Zero-Touch-Registrierung</li><li>• Aktivieren von mehreren Geräten mit Knox Mobile Enrollment</li><li>• Aktivieren von beim DEP registrierten iOS-Geräten</li><li>• Aktivieren von iOS-Geräten mit Apple Configurator 2</li></ul>
4	Aktualisieren Sie die Vorlage für die Aktivierungs-E-Mail.
5	Erstellen Sie ein Aktivierungsprofil, und weisen Sie es Benutzerkonten oder Benutzergruppen zu.
6	Senden einer Aktivierungs-E-Mail an mehrere BenutzerSenden Sie eine Aktivierungs-E-Mail an einen bestimmten Benutzer, oder lassen Sie zu, dass Benutzer Aktivierungskennwörter in UEM Self-Service festlegen.

Schritt	Aktion
7	<p>Senden Sie Aktivierungsanweisungen an Benutzer:</p> <ul style="list-style-type: none"> <li>• Aktivieren von Android-Geräten</li> <li>• Aktivieren von iOS-Geräten</li> <li>• Aktivieren eines macOS- oder Apple TV-Geräts mit BlackBerry UEM Self-Service</li> <li>• Aktivieren eines Windows 10-Tablets oder -Computers</li> </ul>

## Aktivierungsarten: iOS-Geräte

Aktivierungsart	Beschreibung
MDM-Steuerelemente	<p>Die Aktivierungsart stellt eine grundlegende Geräteverwaltung mithilfe der durch iOS und iPadOS verfügbaren Gerätesteuerelemente bereit. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten.</p> <p>Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern. Während der Aktivierung müssen Benutzer ein Mobilgeräteverwaltungsprofil auf ihrem Gerät installieren.</p> <p>Um festzulegen, ob BlackBerry UEM die Aktivierung anhand der Geräte-ID einschränken kann, wählen Sie „Nur genehmigte Geräte-IDs zulassen“ aus.</p>

Aktivierungsart	Beschreibung
Privatsphäre des Benutzers	<p>Diese Aktivierungsart bietet die grundlegende Steuerung von Geräten und stellt gleichzeitig sicher, dass die persönlichen Daten des Benutzers privat bleiben. Auf dem Gerät ist kein separater Container installiert, und es wird keine zusätzliche Sicherheit für geschäftliche Daten geboten. Geräte können Dienste wie Find my Phone und Root Detection nutzen. Administratoren können jedoch keine Geräterichtlinien steuern.</p> <p><b>Hinweis:</b> Um die Lizenzierung auf SIM-Basis zuzulassen, müssen Sie die Option „Zugriff auf SIM-Karten- und Hardwareinformationen zulassen, um die SIM-basierte Lizenzierung zu aktivieren“ im Aktivierungsprofil auswählen. Benutzer müssen ein MDM-Profil installieren, das nur auf die SIM-Karten- und Hardwareinformationen zugreifen kann, die erforderlich sind, um zu prüfen, ob eine entsprechende SIM-Lizenz verfügbar ist (z. B. ICCID und IMEI).</p> <p>Diese Aktivierungsart wird für Apple TV-Geräte nicht unterstützt.</p> <p>Wenn Sie Privatsphäre des Benutzers-Aktivierungen zulassen, wählen Sie die Profile aus, die Sie basierend auf den Anforderungen Ihres Unternehmens auf dem Gerät verwalten möchten. Sie können eine der folgenden Optionen auswählen:</p> <ul style="list-style-type: none"> <li>• Zugriff auf SIM-Karten- und Geräte-Hardwareinformationen zulassen, um die SIM-basierte Lizenzierung zu aktivieren: Mit dieser Option wird festgelegt, ob UEM auf SIM-Karten- und Geräte-Hardwareinformationen wie ICCID und IMEI zugreifen kann, um zu überprüfen, ob eine entsprechende SIM-Lizenz verfügbar ist.</li> <li>• App-Verwaltung zulassen: Mit dieser Option wird festgelegt, ob Sie geschäftliche Apps auf dem Gerät installieren oder entfernen und eine Liste der installierten geschäftlichen Apps auf dem Bildschirm mit den Benutzerdetails anzeigen möchten. Sie können auch angeben, ob App-Verknüpfungen zugelassen werden sollen.</li> <li>• IT-Richtlinienverwaltung zulassen: Mit dieser Option wird festgelegt, ob Sie einen begrenzten Satz von IT-Richtlinienregeln auf das Gerät anwenden möchten (Kennwortrichtlinien, Screenshots zulassen, Dokumente aus verwalteten Quellen in nicht verwalteten Zielen zulassen und Dokumente aus nicht verwalteten Quellen in verwalteten Zielen zulassen).</li> <li>• E-Mail-Profilverwaltung zulassen: Mit dieser Option wird festgelegt, ob die E-Mail-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen.</li> <li>• Wi-Fi-Profilverwaltung zulassen: Mit dieser Option wird festgelegt, ob die Wi-Fi-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen.</li> <li>• VPN-Profilverwaltung zulassen: Mit dieser Option wird festgelegt, ob die VPN-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen.</li> </ul>

Aktivierungsart	Beschreibung
Benutzerdatenschutz - Benutzerregistrierung	<p>Diese Aktivierungsart kann für iOS- und iPadOS-Geräte verwendet werden, um sicherzustellen, dass Benutzerdaten privat und von geschäftlichen Daten getrennt bleiben. Ein separater geschäftlicher Bereich auf dem Gerät wird für geschäftliche Apps und native Notizen, iCloud Drive, E-Mails (Anhänge und vollständige E-Mail-Texte), Kalender (Anhänge) und iCloud Keychain-Apps installiert.</p> <p>Diese Aktivierungsart ermöglicht die Verwendung von App-Verwaltung, IT-Richtlinienverwaltung, E-Mail-Profilen Wi-Fi-Profilen und „VPN pro App“.</p> <p>Administratoren können geschäftliche Daten verwalten (z. B. geschäftliche Daten löschen), ohne dass Auswirkungen auf persönliche Daten erfolgen.</p> <p>Diese Aktivierungsart wird für iPhone- und iPad-Geräte unterstützt.</p>
Geräteregistrierung nur für BlackBerry 2FA	<p>Diese Aktivierungsart unterstützt die BlackBerry 2FA-Lösung für Geräte, die nicht von 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.</p> <p>Wenn ein Gerät aktiviert ist, können Sie begrenzte Geräteinformationen in der Verwaltungskonsole anzeigen. Außerdem können Sie das Gerät über einen Befehl deaktivieren.</p> <p>Diese Aktivierungsart wird nur für Microsoft Active Directory-Benutzer unterstützt. Sie wird für Apple TV-Geräte nicht unterstützt.</p> <p>Weitere Informationen finden Sie in der <a href="#">Dokumentation zu BlackBerry 2FA</a>.</p>

## Aktivierungsarten: Android-Geräte

Bei Android-Geräten 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 Samsung Knox Workspace nicht unterstützen, die zweite.

### Android Management-Geräte

Bevor Sie Geräte mit Android Management-Aktivierungsarten aktivieren, lesen Sie die [Überlegungen zu Aktivierungsarten für Android Management](#).

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Benutzer-Datenschutz (Android Management mit geschäftlichem Profil)	<p>Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit Befehlen und IT-Richtlinienregeln. Auf dem Gerät wird ein Arbeitsprofil erstellt, das geschäftliche und persönliche Daten trennt. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt.</p>

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Management-Gerät mit geschäftlichem Profil)	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Auf dem Gerät wird ein Arbeitsprofil erstellt, das geschäftliche und persönliche Daten trennt. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstützt die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in UEM-Protokolldateien.</p> <p>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.</p> <p>Für diese Aktivierungsart muss das Gerät vor seiner Aktivierung auf Werkseinstellungen zurückgesetzt werden. Wenn BlackBerry UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt.</p>
Nur geschäftlicher Bereich (vollständig verwaltetes Android Management-Gerät)	<p>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.</p> <p>Während der Aktivierung installiert das Gerät UEM Client automatisch und gewährt Administratorberechtigungen. Benutzer können die Administratorberechtigungen nicht aufheben oder die App deinstallieren.</p> <p>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.</p> <p>Für diese Aktivierungsart muss das Gerät vor seiner Aktivierung auf Werkseinstellungen zurückgesetzt werden. Wenn UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt.</p>

## Android Enterprise-Geräte

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise mit geschäftlichem Profil)	<p>Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit Befehlen und IT-Richtlinienregeln. Auf dem Gerät wird ein Arbeitsprofil erstellt, das geschäftliche und persönliche Daten trennt. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt.</p> <p>Um die Google Play-App-Verwaltung für Android Enterprise-Geräte zuzulassen, wählen Sie „Google Play zum Workspace hinzufügen“ im Aktivierungsprofil aus (standardmäßig aktiviert). Wenn das Gerät keinen Zugriff auf Google Play hat, muss der Benutzer die neueste Version von UEM Client von einer anderen Quelle herunterladen. Informationen zum Download der .apk-Datei des neuesten UEM Client finden Sie in <a href="#">KB 42607</a>.</p> <p>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.</p> <p>Die Benutzer müssen dem UEM Client keine Administratorberechtigungen erteilen.</p>
Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil)	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Auf dem Gerät wird ein Arbeitsprofil erstellt, das geschäftliche und persönliche Daten trennt. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstützt die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in UEM-Protokolldateien.</p> <p>Um die Google Play-App-Verwaltung für Android Enterprise-Geräte zuzulassen, wählen Sie „Google Play zum geschäftlichen Bereich hinzufügen“ im Aktivierungsprofil aus (standardmäßig aktiviert).</p> <p>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.</p> <p>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.</p> <p>Um festzulegen, ob UEM die Aktivierung anhand der Geräte-ID einschränken kann, wählen Sie im Aktivierungsprofil „Nur genehmigte Geräte-IDs zulassen“ aus.</p> <p>Für diese Aktivierungsart muss das Gerät vor seiner Aktivierung auf Werkseinstellungen zurückgesetzt werden. Wenn UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt.</p> <p>Während der Aktivierung müssen Benutzer dem UEM Client Administratorberechtigungen erteilen.</p>

Aktivierungsart	Beschreibung
<p>Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)</p>	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Dabei 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.</p> <p>Um die Google Play-App-Verwaltung für Android Enterprise-Geräte zuzulassen, wählen Sie „Google Play zum Workspace hinzufügen“ im Aktivierungsprofil aus (standardmäßig aktiviert). Wenn das Gerät keinen Zugriff auf Google Play hat, kann der Benutzer den UEM Client mithilfe einer .apk -Datei der App herunterladen. Sie können einen QR Code konfigurieren und aufnehmen, der den Speicherort der Quelldatei von UEM Client in der Aktivierungs-E-Mail enthält, die Sie an Benutzer senden. Wenn ein Benutzer den QR Code scannt, wird der UEM Client automatisch heruntergeladen.</p> <p>Um einen QR Code zu konfigurieren und in die Aktivierungs-E-Mail-Nachricht aufzunehmen, müssen Sie das Kontrollkästchen „QR-Codes für Geräteaktivierung zulassen“ auf der Seite „Standardeinstellungen für die Aktivierung“ aktivieren (Einstellungen &gt; Allgemeine Einstellungen &gt; Standardeinstellungen für die Aktivierung). Sie müssen auch das Kontrollkästchen „Zulassen, dass der QR-Code den Speicherort der Quelldatei der UEM Client-App enthält“ aktivieren und den Speicherort der Quelldatei der UEM Client-App angeben. Informationen zum Erhalt der .apk-Datei der neuesten Version von UEM Client finden Sie in <a href="#">KB 42607</a>.</p> <p>Während der Aktivierung installiert das Gerät UEM Client automatisch und gewährt Administratorberechtigungen. Benutzer können die Administratorberechtigungen nicht aufheben oder die App deinstallieren.</p> <p>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.</p> <p>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.</p> <p>Um festzulegen, ob UEM die Aktivierung anhand der Geräte-ID einschränken kann, wählen Sie im Aktivierungsprofil „Nur genehmigte Geräte-IDs zulassen“ aus.</p> <p>Für diese Aktivierungsart muss das Gerät vor seiner Aktivierung auf Werkseinstellungen zurückgesetzt werden. Wenn UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt.</p>

### Android-Geräte ohne geschäftliches Profil

Die folgenden Aktivierungsarten gelten für alle Android-Geräte.

Aktivierungsart	Beschreibung
Privatsphäre des Benutzers	<p>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. Auf dem Gerät wird kein separater Container erstellt. 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.</p> <p>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.</p>
Geräteregistrierung nur für BlackBerry 2FA	<p>Diese Aktivierungsart unterstützt die BlackBerry 2FA-Lösung für Geräte, die nicht von 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.</p> <p>Wenn ein Gerät aktiviert ist, können Sie begrenzte Geräteinformationen in der Verwaltungskonsole anzeigen. Außerdem können Sie das Gerät über einen Befehl deaktivieren.</p> <p>Diese Aktivierungsart wird nur für Microsoft Active Directory-Benutzer unterstützt.</p> <p>Weitere Informationen <a href="#">finden Sie in der Dokumentation zu BlackBerry 2FA</a>.</p>

### Samsung Knox Workspace-Geräte

**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 [KB 54614](#).

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Benutzer-Datenschutz - (Samsung Knox)	<p>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. Auf dem Gerät wird ein separater geschäftlicher Bereich erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich 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.</p> <p>Während der Aktivierung müssen Benutzer dem UEM Client Administratorberechtigungen erteilen.</p>

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und die Knox MDM- sowie Knox Workspace IT-Richtlinienregeln. Auf dem Gerät wird ein separater geschäftlicher Bereich erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich zuzugreifen. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt.</p> <p>Während der Aktivierung müssen Benutzer dem UEM Client Administratorberechtigungen erteilen.</p>

## Aktivierungsarten: macOS-Geräte

Aktivierungsart	Beschreibung
MDM-Steuerelemente	<p>Diese Aktivierungsart ermöglicht die grundlegende Geräteverwaltung über die von macOS zur Verfügung gestellten Gerätesteuererelemente.</p> <p>Wenn ein Benutzer ein macOS-Gerät aktiviert, werden das Gerät und der Benutzer als separate Einheiten auf BlackBerry UEM eingerichtet. Zwischen UEM und dem Gerät und UEM und dem Benutzerkonto werden separate Kommunikationskanäle eingerichtet, sodass Sie das Gerät und den Benutzer getrennt verwalten können. Einige Profile werden nur dem Benutzer zugewiesen (z. B. E-Mail-Profil). Einige Profile werden nur dem Gerät zugewiesen (z. B. Proxy-Profil). Bei manchen Profilen können Sie wählen, ob das Profil für das Gerät oder den Benutzer gelten soll (zum Beispiel Wi-Fi-Profil).</p> <p>Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern. Benutzer aktivieren macOS-Geräte mithilfe von BlackBerry UEM Self-Service.</p>

## Aktivierungsarten: Windows 10-Geräte

**Hinweis:** Windows 10 Mobile-Geräte werden [von Microsoft nicht mehr unterstützt](#) und auf UEM nur eingeschränkt unterstützt.

Aktivierungsart	Beschreibung
MDM-Steuerelemente	<p>Diese Aktivierungsart stellt eine grundlegende Geräteverwaltung über die von Windows 10-Geräten zur Verfügung gestellten Gerätesteuererelemente bereit. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten.</p> <p>Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern. Benutzer von Windows 10 aktivieren Geräte über die Windows 10-App für den geschäftlichen Zugriff.</p>

# Verwalten von Aktivierungseinstellungen

Sie können festlegen, wie Benutzer Geräte aktivieren, z. B. ob Benutzer ein Aktivierungskennwort eingeben müssen, ob sie einen QR Code scannen müssen, die Gültigkeitsdauer eines Aktivierungskennworts oder QR Code und ob Benutzer mehrere Geräte mit demselben Kennwort oder QR Code aktivieren können.

## Konfigurieren der standardmäßigen Aktivierungseinstellungen

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Einstellungen > Allgemeine Einstellungen > Aktivierungsstandards**.
2. Geben Sie im Abschnitt **Geräteaktivierungsstandards** das Aktivierungskennwort und die QR Code-Optionen an.
3. Wenn BlackBerry UEM einen Benutzer bei jeder Aktivierung eines Geräts in seinem Konto per E-Mail benachrichtigen soll, aktivieren Sie das Kontrollkästchen **Geräteaktivierte Benachrichtigung senden**.
4. Um Benutzern die Aktivierung von BlackBerry Dynamics-Apps mit einem QR Code zu ermöglichen, aktivieren Sie im Abschnitt **Standardmäßige BlackBerry Dynamics-Appsteuerung** das Kontrollkästchen **QR-Codes für das Entsperren von BlackBerry Dynamics-Apps verwenden**. Weitere Informationen finden Sie unter [Generieren von Zugriffsschlüsseln, Aktivierungskennwörtern oder QR-Codes für BlackBerry Dynamics-Apps](#).
5. Um die Aktivierung ihrer Mobilgeräte durch Benutzer zu vereinfachen, aktivieren Sie im Abschnitt **BlackBerry Infrastructure** das Kontrollkästchen **Registrierung mit BlackBerry Infrastructure einschalten**. Wenn Sie diese Option löschen, werden die Benutzer bei der Aktivierung von Geräten aufgefordert, die Serveradresse für UEM anzugeben.
6. Um eine Liste genehmigter Geräte-IDs zu importieren oder zu exportieren, klicken Sie im Abschnitt **Importieren oder Exportieren einer Liste genehmigter Geräte-IDs** auf **Durchsuchen**. Navigieren Sie zu der CSV-Datei, die eine Liste genehmigter Geräte-IDs beinhaltet, und wählen Sie sie aus. Weitere Informationen finden Sie unter [Importieren oder Exportieren einer Liste genehmigter Geräte-IDs](#).
7. Klicken Sie auf **Speichern**.

## Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail-Nachricht

Sie können ein Aktivierungskennwort einrichten und einem Benutzer eine Aktivierungs-E-Mail mit den Anweisungen zur Aktivierung von Geräten senden. In lokalen Umgebungen wird die E-Mail-Nachricht von der E-Mail-Adresse gesendet, die Sie in den SMTP-Servereinstellungen konfiguriert haben.

**Bevor Sie beginnen:** [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach dem Namen eines Benutzerkontos, und klicken Sie darauf.
3. Klicken Sie im Abschnitt **Aktivierungsdetails** auf **Aktivierungskennwort festlegen**.
4. Führen Sie in der Dropdown-Liste **Aktivierungsoption** eine der folgenden Optionen aus:
  - Wenn Sie möchten, dass der Benutzer sein Gerät mit dem ihm aktuell zugewiesenen Aktivierungsprofil aktiviert, wählen Sie **Standardmäßige Geräteaktivierung** aus.
  - Wenn Sie ein Aktivierungskennwort mit einem bestimmten Aktivierungsprofil verknüpfen möchten, wählen Sie **Geräteaktivierung mit einem bestimmten Aktivierungsprofil** aus. Weitere Informationen finden Sie unter [Aktivierung mehrerer Geräte mit verschiedenen Aktivierungsarten durch Benutzer zulassen](#).
5. Führen Sie in der Dropdown-Liste **Aktivierungskennwort** eine der folgenden Optionen aus:

- Wenn Sie automatisch ein Kennwort erstellen möchten, wählen Sie **Automatisch ein Geräteaktivierungskennwort generieren und eine E-Mail mit Aktivierungsanweisungen senden**. Wenn Sie diese Option auswählen, müssen Sie eine E-Mail-Vorlage auswählen, mit der die Informationen an den Benutzer gesendet werden sollen.
  - Wenn Sie ein Aktivierungskennwort für den Benutzer festlegen und ggf. eine Aktivierungs-E-Mail senden möchten, wählen Sie **Geräteaktivierungskennwort festlegen** aus, und geben Sie ein Kennwort ein.
6. Optional können Sie den Ablauf des Aktivierungszeitraums ändern, um anzugeben, wie lange das Aktivierungskennwort gültig bleibt.
  7. Wenn Sie möchten, dass das Aktivierungskennwort nur für eine Geräteaktivierung gültig ist, wählen Sie **Aktivierungszeitraum endet nach der Aktivierung des ersten Geräts** aus.
  8. Wählen Sie in der Dropdown-Liste **Vorlage für Aktivierungs-E-Mail** die E-Mail-Vorlage aus, die Sie kopieren möchten.
  9. Klicken Sie auf **Submit**.

## Senden einer Aktivierungs-E-Mail an mehrere Benutzer

Sie können Aktivierungs-E-Mail-Nachrichten an mehrere Benutzer auf einmal senden. Wenn Sie eine Aktivierungs-E-Mail an mehrere Benutzer senden, wird das Aktivierungskennwort automatisch generiert. Die E-Mail wird von der E-Mail-Adresse gesendet, die Sie in den SMTP-Servereinstellungen konfiguriert haben.

**Bevor Sie beginnen:** [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben jedem Benutzer, der die Aktivierungs-E-Mail erhalten soll.
3. Klicken Sie auf .
4. Führen Sie in der Dropdown-Liste **Aktivierungsoption** eine der folgenden Optionen aus:
  - Wenn Sie möchten, dass Benutzer ihre Geräte mit dem ihnen aktuell zugewiesenen Aktivierungsprofil aktivieren, wählen Sie **Standardmäßige Geräteaktivierung** aus.
  - Wenn Sie ein Aktivierungskennwort mit einem bestimmten Aktivierungsprofil verknüpfen möchten, wählen Sie **Geräteaktivierung mit einem bestimmten Aktivierungsprofil** aus. Weitere Informationen zum Verknüpfen von Aktivierungskennwörtern mit Aktivierungsprofilen finden Sie unter [Aktivierung mehrerer Geräte mit verschiedenen Aktivierungsarten durch Benutzer zulassen](#).
5. Wählen Sie in der Dropdown-Liste **Aktivierungskennwort** die Option **Automatisch ein Geräteaktivierungskennwort generieren und eine E-Mail mit Aktivierungsanweisungen senden** aus.
6. Sie können den Ablauf des Aktivierungszeitraums ändern, um anzugeben, wie lange das Aktivierungskennwort gültig bleibt.
7. Wenn Sie möchten, dass das Aktivierungskennwort nur für eine Geräteaktivierung gültig ist, wählen Sie **Aktivierungszeitraum endet nach der Aktivierung des ersten Geräts** aus.
8. Wählen Sie in der Dropdown-Liste **Vorlage für Aktivierungs-E-Mail** die E-Mail-Vorlage aus, die Sie kopieren möchten.
9. Klicken Sie auf **Senden**.

## Zulassen, dass Benutzer Aktivierungskennwörter festlegen in BlackBerry UEM Self-Service

Sie können zulassen, dass Benutzer mit iOS-, Android- und Windows-Geräten ihre eigenen Aktivierungskennwörter über BlackBerry UEM Self-Service erstellen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Self-Service > Self-Service-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen **Benutzern die Geräteaktivierung in der Self-Service-Konsole gestatten**, und führen Sie die folgenden Schritte aus:
3. Geben Sie an, wie viel Zeit ein Benutzer hat, um ein Gerät zu aktivieren, bevor das Aktivierungskennwort abläuft.
4. Geben Sie die Mindestanzahl von Zeichen an, die für ein Aktivierungskennwort erforderlich sind.
5. Wählen Sie in der Dropdown-Liste **Mindestkomplexität des Kennworts** die erforderliche Komplexität aus.
6. Um automatisch eine Aktivierungs-E-Mail an Benutzer zu senden, wenn sie ein Aktivierungskennwort erstellen, aktivieren Sie das Kontrollkästchen **Aktivierungs-E-Mail senden**. Wählen Sie in der Dropdown-Liste **Aktivierungs-E-Mail-Vorlage** eine E-Mail-Vorlage aus.
7. Um benutzerdefinierte Aktivierungsnachrichten an Benutzer zu senden, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Aktivierungsnachrichten senden**. Wählen Sie eine Nachrichtenvorlage für jeden Gerätetyp aus der entsprechenden Dropdown-Liste aus.
8. Um dem Benutzer jedes Mal, wenn er sich bei UEM Self-Service anmeldet, eine Anmeldebenachrichtigungs-E-Mail zu senden, aktivieren Sie das Kontrollkästchen **Benachrichtigung für Self-Service-Anmeldung senden**.
9. Klicken Sie auf **Speichern**.

## Aktivierung mehrerer Geräte mit verschiedenen Aktivierungsarten durch Benutzer zulassen

Sie können mehrere Aktivierungskennwörter für einen Benutzer erstellen und diese mit bestimmten Aktivierungsprofilen verknüpfen, damit Benutzer Geräte mit verschiedenen Aktivierungsarten aktivieren können.

Sie können z. B. einstellen, dass Benutzer geschäftliche Geräte mit einer Aktivierungsart aktivieren, bei der Sie vollständige Kontrolle über die Geräte haben, ihre persönlichen Geräte jedoch mit einer Aktivierungsart aktivieren, die für Benutzerdatenschutz sorgt. Durch die Verknüpfung eines Aktivierungskennworts mit einem Aktivierungsprofil, das eine vollständige Gerätekontrolle ermöglicht, und einem zweiten Aktivierungskennwort mit Benutzerdatenschutz-Aktivierungsprofil können Benutzer jedes Gerät mit verschiedenen Ergebnissen aktivieren. Sie können E-Mail-Vorlagen erstellen, in denen der Verwendungszweck jedes Kennworts erklärt wird.

Um ein Aktivierungskennwort mit einem bestimmten Aktivierungsprofil zu verknüpfen, wenn Sie ein Benutzerkonto erstellen oder eine Aktivierungs-E-Mail senden, wählen Sie die Option „Geräteaktivierung mit einem bestimmten Aktivierungsprofil“ aus.

Sie können über maximal zwei Aktivierungskennwörter verfügen, die mit bestimmten Aktivierungsprofilen verknüpft sind. Jedes Kennwort kann zur Aktivierung mehrerer Geräte verwendet werden. Beachten Sie, dass bei Aktivierungskennwörtern, die mit Aktivierungsprofilen verknüpft sind, die Option „Anzahl der Geräte, die ein Benutzer aktivieren kann“ im Aktivierungsprofil nicht erzwungen wird.

Wenn Sie ein Aktivierungsprofil löschen, mit dem ein Aktivierungskennwort verknüpft ist, läuft das Aktivierungskennwort automatisch ab. Sie können die Aktivierungskennwörter eines Benutzers bei Bedarf jederzeit [ablaufen lassen](#).

Benutzer können keine Aktivierungskennwörter erstellen, die mit bestimmten Aktivierungsprofilen in BlackBerry UEM Self-Service verknüpft sind.

Diese Option wird von iOS-Geräten mit DEP-Registrierung nicht unterstützt.

## Erzwingen des Ablaufens von Aktivierungskennwörtern

Sie können das Ablaufen eines für einen Benutzer erstellten Aktivierungskennworts manuell erzwingen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach dem Namen eines Benutzerkontos, und klicken Sie darauf.
3. Klicken Sie im Abschnitt **Aktivierungsdetails** unter dem Aktivierungskennwort, das Sie ablaufen lassen möchten, auf **Ablaufen**.

Das Aktivierungskennwort läuft sofort ab. Wenn Sie erzwingen, dass ein reguläres Aktivierungskennwort abläuft, werden Uhrzeit und Datum des Kennwortablaufs angezeigt. Wenn Sie das Ablaufen eines Aktivierungskennworts erzwingen, das mit einem bestimmten Aktivierungsprofil gekoppelt war, werden die Details des Geräteaktivierungskennworts nicht mehr angezeigt.

# Unterstützung von Android Enterprise- und Android Management-Aktivierungen

Die Art und Weise, wie Sie Android Enterprise- und Android Management-Geräte von Benutzern aktivieren, hängt von mehreren Faktoren ab, darunter der Android-Betriebssystemversion des Geräts und dem Maß an Kontrolle, den Ihr Unternehmen über die Geräte der Benutzer haben möchte. Sie kann auch davon abhängen, ob Ihr Unternehmen mit Google-Diensten über verwaltete Google Play-Konten, Google Workspace-Domänen oder Google Cloud-Domänen interagiert oder ob es keine Google-Dienste verwendet.

## Unterstützung von Android Enterprise- und Android Management-Aktivierungen mithilfe verwalteter Google Play-Konten

Wenn Ihr Unternehmen keine Google-Domäne hat oder wenn Sie BlackBerry UEM nicht mit Ihrer Google-Domäne verbinden möchten, können Sie Android Enterprise- und Android Management-Geräte mit verwalteten Google Play-Konten aktivieren. Mithilfe verwalteter Google Play-Konten können Sie interne Apps zu Google Play hinzufügen, die Android Enterprise-Gerätebenutzer herunterladen können.

Wenn Sie verwaltete Google Play-Konten mit UEM verwenden, können Sie die Verbindung zwischen UEM und Google über ein beliebiges Google- oder Gmail-Konto herstellen. Es werden keine personenbezogenen Daten über Ihre Benutzer an Google gesendet. Nachdem Sie eine Verbindung zwischen UEM und Google hergestellt haben, können Sie Benutzern die Aktivierung von Android Enterprise- und Android Management-Geräten und das Herunterladen geschäftlicher Apps mit Google Play gestatten. Weitere Informationen zum Konfigurieren von UEM für die Unterstützung von Android Enterprise- und Android Management-Geräten finden Sie unter [Konfigurieren von BlackBerry UEM zur Unterstützung von Android Enterprise-Geräten](#) und [Konfigurieren von BlackBerry UEM zur Unterstützung von Android Management-Geräten](#).

## Unterstützen von Android Enterprise-Aktivierungen mit einer Google Workspace-Domäne

Wenn Sie BlackBerry UEM für eine Verbindung mit der Google Workspace-Domäne Ihres Unternehmens konfiguriert haben, müssen Sie die folgenden Aufgaben ausführen, bevor Benutzer Android Enterprise-Geräte aktivieren.

**Bevor Sie beginnen:** [Konfigurieren von BlackBerry UEM zur Unterstützung von Android Enterprise-Geräten](#).

1. Erstellen Sie in der Google Workspace-Domäne Benutzerkonten für die Android-Benutzer.
2. Wählen Sie die Einstellung **EMM-Richtlinie erzwingen**.  
Diese Einstellung ist für Geräte, denen die Aktivierungsarten Nur geschäftlicher Bereich und Geschäftlich und persönlich – vollständige Kontrolle zugewiesen wird, 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. Erstellen Sie in UEM lokale Benutzerkonten für die Android-Benutzer. Die E-Mail-Adressen der einzelnen Konten müssen mit denen der zugehörigen Google Workspace-Konten übereinstimmen.
4. Weisen Sie in 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 von BlackBerry UEM zur Unterstützung von Android Enterprise-Geräten](#). Wenn Sie UEM für die Verbindung mit einer Google Cloud-Domäne konfigurieren, müssen Sie auswählen, ob 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.

1. Fügen Sie in UEM Verzeichnis-Benutzerkonten für die Android Enterprise-Benutzer hinzu.
2. Wenn Sie nicht zulassen, dass UEM in Ihrer Google Cloud-Domäne Benutzerkonten erstellt, müssen Sie in der Google Cloud-Domäne und in UEM Benutzerkonten erstellen. Führen Sie einen der folgenden Schritte 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 UEM-Benutzerkonten übereinstimmen. Stellen Sie sicher, dass Ihre Android Enterprise-Benutzer das Kennwort für ihre Google Cloud-Konten kennen.
  - Synchronisieren Sie mit 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 die Aktivierungsart 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 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. Sie können einen bestimmten Download-Speicherort in einen QR Code aufnehmen.
- Geräte, die mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz aktiviert werden, müssen nicht auf die Werkseinstellungen zurückgesetzt werden. Bei diesen Geräten kann der Benutzer nach Abschluss der vorkonfigurierten Einrichtung den UEM Client installieren.

Informationen zum Download der .apk-Datei des neuesten UEM Client finden Sie in [KB 42607](#).

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

Anforderungen	Beschreibung
BlackBerry UEM - Umgebung	Wenn Sie nur Geräte unterstützen möchten, die keinen Zugriff auf Google Play haben, müssen Sie Ihre UEM-Umgebung nicht mit Android Enterprise integrieren. Wenn jedoch Geräte mit und ohne Zugriff auf Google Play unterstützt werden sollen, müssen Sie Ihre Umgebung in Android Enterprise integrieren.
Standardmäßige Aktivierungseinstellungen	<p>Wenn Sie den UEM Client-Standort in einen QR-Code aufnehmen möchten, wählen Sie in den <a href="#">standardmäßigen Aktivierungseinstellungen</a> die Optionen „Zulassen, dass der QR-Code den Speicherort der Quelldatei der UEM Client-App enthält“ und „Standardspeicherort verwenden“ aus.</p> <p>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.</p>
Aktivierungsprofileinstellungen	<p>Überprüfen Sie die folgenden Einstellungen im Aktivierungsprofil:</p> <ul style="list-style-type: none"> <li>• Deaktivieren Sie die Option „Google Play-Konto zu geschäftlichem Bereich hinzufügen“.</li> <li>• 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.</li> </ul>
IT-Richtlinienregeln	Für Benutzer, denen die Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) zugewiesen wurde, um die Installation von Apps außerhalb von Google Play zuzulassen, aktivieren Sie die IT-Richtlinienregel „Installation von Apps, die nicht von Google Play stammen, zulassen“.
Nicht-BlackBerry Dynamics-Apps	<p>Fügen Sie Nicht-BlackBerry Dynamics-Apps als interne Apps zu UEM hinzu, und ordnen Sie sie den entsprechenden Benutzern zu.</p> <ol style="list-style-type: none"> <li>1. Besorgen Sie die APK-Dateien der Apps, die Sie zuweisen möchten.</li> <li>2. Klicken Sie in der Menüleiste der Verwaltungskonsole auf <b>Apps</b>.</li> <li>3. Klicken Sie auf  &gt; <b>Interne Apps</b>.</li> <li>4. Klicken Sie auf <b>Durchsuchen</b>, und wählen Sie die APK-Datei aus.</li> <li>5. Wählen Sie im Feld <b>Senden an</b> die Option <b>Alle Android-Geräte</b> aus.</li> <li>6. Deaktivieren Sie die Option <b>App in Google-Domäne veröffentlichen</b>.</li> <li>7. Klicken Sie auf <b>Hinzufügen</b>.</li> <li>8. Wiederholen Sie die zuvor genannten Schritte für jede App, die Sie hinzufügen möchten.</li> <li>9. Weisen Sie die Apps Benutzern zu. Die App-Verfügbarkeit muss auf <b>Erforderlich</b> gesetzt sein.</li> </ol>

Anforderungen	Beschreibung
BlackBerry Dynamics-Apps	<p>Laden Sie für BlackBerry Dynamics-Apps die interne App-Quelldatei hoch, und weisen Sie die App Benutzern zu.</p> <p>Um interne Apps auf Geräten, die keinen Zugriff auf Google Play haben, zu installieren oder zu aktualisieren, tun Sie Folgendes:</p> <ol style="list-style-type: none"> <li>1. Besorgen Sie die APK-Dateien der BlackBerry Dynamics-Apps, die Sie zuweisen möchten.</li> <li>2. Klicken Sie in der Menüleiste der Verwaltungskonsole auf <b>Apps</b>.</li> <li>3. Klicken Sie auf eine BlackBerry Dynamics-App.</li> <li>4. Klicken Sie auf die Registerkarte <b>Android</b>.</li> <li>5. Klicken Sie auf <b>Quelldatei für interne App hinzufügen</b>.</li> <li>6. Klicken Sie auf <b>Durchsuchen</b>, und wählen Sie die APK-Datei aus.</li> <li>7. Klicken Sie auf <b>Hinzufügen</b>.</li> <li>8. Klicken Sie auf <b>Speichern</b>.</li> <li>9. Wiederholen Sie die zuvor genannten Schritte für jede App, die Sie hinzufügen möchten.</li> <li>10. Weisen Sie die Apps Benutzern zu. Die App-Verfügbarkeit muss auf <b>Erforderlich</b> gesetzt sein.</li> </ol>
BlackBerry UEM Client-App aktualisieren	<p>Um die UEM Client-App auf Geräten zu aktualisieren, müssen Benutzer die neueste Version der APK-Datei manuell herunterladen und installieren.</p>

# Unterstützen von Windows 10-Aktivierungen

Sie können Benutzer bei der Aktivierung der Windows 10-Geräte wie folgt unterstützen:

- Erstellen oder Bearbeiten einer Vorlage für Aktivierungs-E-Mails zur Bereitstellung von Windows 10-Aktivierungsinformation. Weitere Informationen finden Sie unter [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).
- [UEM mit Entra ID Join integrieren](#): Wenn die Entra ID-Einbindung konfiguriert ist, können Benutzer ihre Geräte nur mit ihrem Entra ID-Benutzernamen und -Kennwort aktivieren.
- [Konfigurieren von Windows Autopilot](#): Wenn Sie Windows Autopilot konfigurieren, ist die Registrierung Teil der vorkonfigurierten Einrichtungserfahrung, und das Gerät wird automatisch aktiviert, wenn der Benutzer sie nur mit seinem Entra ID-Benutzernamen und -Kennwort abschließt.
- [Bereitstellen eines Suchdienstes](#): Sie können eine Java-Web-App von BlackBerry als Suchdienst verwenden, um den Aktivierungsvorgang für Benutzer mit Windows 10-Geräten zu vereinfachen. Wenn Sie den Suchdienst verwenden, müssen Sie während des Aktivierungsvorgangs keine Serveradresse eingeben.

# Unterstützung der Apple-Benutzerregistrierung auf iOS- und iPadOS-Geräten

Sie können die Aktivierungsart Benutzerdatenschutz - Benutzerregistrierung für iOS- und iPadOS-Geräte verwenden, um sicherzustellen, dass Benutzerdaten privat und von geschäftlichen Daten getrennt bleiben. Bei dieser Aktivierungsart wird ein separater geschäftlicher Bereich auf dem Gerät für geschäftliche Apps und native Notizen, iCloud Drive, E-Mails (Anhänge und vollständige E-Mail-Texte), Kalender (Anhänge) und iCloud Keychain-Apps installiert. Diese Aktivierungsart ermöglicht die Verwendung von App-Verwaltung, IT-Richtlinienverwaltung, E-Mail-Profilen Wi-Fi-Profilen und „VPN pro App“. Administratoren können geschäftliche Daten verwalten (z. B. geschäftliche Daten löschen), ohne dass Auswirkungen auf persönliche Daten erfolgen. Diese Aktivierungsart wird auf nicht überwachten iPhone- und iPad-Geräten unterstützt, auf denen unterstützte Versionen von iOS bzw. iPadOS ausgeführt werden.

Wenn die Apple-Benutzerregistrierung unterstützt werden soll, tun Sie Folgendes:

- Stellen Sie sicher, dass die Geräte, die Sie mit dieser Aktivierungsart aktivieren, nicht überwacht werden.
- Erstellen Sie für jeden Benutzer ein verwaltetes Apple-ID-Konto. Die E-Mail-Adresse der verwalteten Apple-ID muss mit der E-Mail-Adresse des Benutzers in BlackBerry UEM übereinstimmen.
- Wenn Sie das Geräteaktivierungskennwort für einen Benutzer festlegen, wählen Sie die E-Mail-Vorlage für die Aktivierung der Apple-Benutzerregistrierung aus.
- Wenn Sie Benutzern erlauben möchten, andere BlackBerry Dynamics-Apps einfach zu aktivieren, Zertifikate zu importieren, BlackBerry 2FA-Funktionen zu verwenden, CylancePROTECT zu verwenden und ihren Konformitätsstatus zu überprüfen, weisen Sie den BlackBerry UEM Client mit einer VPP-Lizenz zu. Wenn Sie die Verfügbarkeit auf „Erforderlich“ setzen, wird der Benutzer aufgefordert, die App zu installieren. Wenn Sie die Verfügbarkeit auf „Optional“ einstellen, muss der Benutzer die App manuell aus den geschäftlichen Apps herunterladen.

# Unterstützung von Samsung Knox DualDAR

Geräte, die Samsung Knox DualDAR-Verschlüsselung unterstützen, können geschäftliche Daten mit zwei Verschlüsselungsschichten sichern. Die äußere Schicht von Knox DualDAR basiert auf dateibasierter Android-Verschlüsselung und wurde durch Samsung zur Unterstützung des MDFPP-Standards erweitert. Im Aktivierungsprofil können Sie angeben, ob Sie die integrierte Standard-Verschlüsselungs-App oder eine interne Verschlüsselungs-App für die innere Verschlüsselungsschicht im Arbeitsprofil verwenden möchten.

Wenn Sie die Standard-App verwenden, wird das Arbeitsprofil mit einem FIPS 140-2-zertifizierten kryptografischen Modul gesichert, das im Samsung Knox-Framework enthalten ist. Die interne Verschlüsselungs-App ist ein speziell entwickeltes Kryptografiemodul, das von Ihrem Unternehmen oder einem Drittanbieter entwickelt wurde und gemäß FIPS 140-2 zertifiziert sein sollte. Wenn der Benutzer das Gerät nicht verwendet, sind alle Daten im Arbeitsprofil gesperrt und können nicht von im Hintergrund ausgeführten Apps aufgerufen werden.

Anforderungen	Beschreibung
Unterstützte Geräte	Flaggschiff-Modelle von Samsung werden unterstützt.
Verschlüsselungs-App	Wenn Sie über eine Verschlüsselungs-App verfügen, die Sie für die Knox DualDAR-Verschlüsselung verwenden möchten, müssen Sie sie als interne App in der Verwaltungskonsole hinzufügen. Sie wählen diese Verschlüsselungs-App aus, wenn Sie ein Aktivierungsprofil für Geräte erstellen, die Knox DualDAR unterstützen. Sie können stattdessen auch die Standard-Verschlüsselungs-App verwenden.
Aktivierungsprofil	<p>Wenn Sie die Knox DualDAR-Verschlüsselung im Aktivierungsprofil aktivieren, sollten Sie das Profil nur Geräten zuweisen, die es unterstützen. Wenn Ihr Unternehmen über eine Gerätemischung verfügt, bei dem nicht klar ist, welche Geräte Knox DualDAR unterstützen, sollten Sie das Aktivierungsprofil einer Gerätegruppe zuweisen. Wenn Sie die Knox DualDAR-Aktivierung für ein nicht unterstütztes Gerät festlegen, wird die Aktivierung nicht erfolgreich abgeschlossen.</p> <p>Zur Unterstützung der Knox DualDAR-Verschlüsselung erstellen Sie ein Aktivierungsprofil mit den folgenden Einstellungen für Android-Geräte:</p> <ul style="list-style-type: none"><li>• Wählen Sie die Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle“ (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil) aus.</li><li>• Aktivieren Sie die Option „Bei der Aktivierung von Android Enterprise-Geräten Premium UEM-Funktionen wie z. B. BlackBerry Secure Connect Plus freischalten“.</li><li>• Wählen Sie die Option „Samsung Knox DualDAR Workspace aktivieren“ aus.</li><li>• Um die standardmäßige Verschlüsselungs-App zu verwenden, wählen Sie die Option „Integrierte Standard-Verschlüsselungs-App“ aus. Wenn Sie eine andere Verschlüsselungs-App verwenden möchten, aktivieren Sie die Option „Interne App für Verschlüsselung auswählen“, und wählen Sie die gewünschte Verschlüsselungs-App aus der App-Liste aus.</li></ul>
BlackBerry UEM Client	Es wird die neueste Version von BlackBerry UEM Client für Android empfohlen.

# Erstellen von Aktivierungsprofilen

Mithilfe von Aktivierungsprofilen können Sie steuern, wie die Geräte aktiviert und verwaltet werden. Ein Aktivierungsprofil gibt die Anzahl der Geräte und Gerätetypen an, die ein Benutzer aktivieren kann, sowie die Aktivierungsart, die für den jeweiligen Gerätetyp verwendet werden soll. Die Aktivierungsart bestimmt, wie viel Kontrolle Sie über aktivierte Geräte haben.

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 Gruppen zuweisen.

## Erstellen eines Aktivierungsprofils

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Richtlinie > Aktivierung**.
2. Klicken Sie auf **+**.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Geben Sie im Feld **Anzahl der Geräte, die ein Benutzer aktivieren kann** die maximale Anzahl von Geräten ein, die ein Benutzer aktivieren kann.
5. Wählen Sie in der Dropdown-Liste **Geräteeigentümer** eine der folgenden Optionen aus:
  - Wenn einige Benutzer persönliche Geräte und einige Benutzer geschäftliche Geräte aktivieren, wählen Sie **Nicht angegeben** aus.
  - Wenn die meisten Benutzer geschäftliche Geräte aktivieren, wählen Sie **Geschäftlich** aus.
  - Wenn die meisten Benutzer persönliche Geräte aktivieren, wählen Sie **Persönlich** aus.
6. Wählen Sie optional in der Dropdown-Liste **Organisationshinweis zuweisen** einen Organisationshinweis 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.
7. Wählen Sie im Abschnitt **Gerätetypen, die Benutzer aktivieren können** die entsprechenden Geräte-OS-Typen aus.
8. Führen Sie für jeden Gerätetyp, den Sie in das Aktivierungsprofil aufnehmen, die folgenden Aktionen aus:
  - 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 Geräte Modelle zulassen:** Benutzer können nur die von Ihnen angegebenen Geräte Modelle aktivieren.
    - **Ausgewählte Geräte Modelle nicht zulassen:** Benutzer können die von Ihnen angegebenen Geräte Modelle nicht aktivieren.
  - Wenn Sie die Geräte Modelle 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.
  - 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.

**Hinweis:** Sie müssen separate Aktivierungsprofile für Android Enterprise und Android Management erstellen. Wenn die Aktivierungsarten Android Enterprise und Android Management im selben Profil angegeben sind, hat die Art Android Management Vorrang, selbst wenn sie niedriger als Android Enterprise eingestuft ist. Nur das Kennwort und die Aktivierungsinformationen für die Aktivierungsart Android Management werden in den QR-Code eingebettet.

**9.** Führen Sie für iOS- und iPadOS-Geräte die folgenden Aktionen durch:

- a) Wenn Sie die Aktivierungsart Privatsphäre des Benutzers auswählen und Sie die SIM-basierte Lizenzierung aktivieren möchten, müssen Sie das Kontrollkästchen **Zugriff auf SIM-Karten- und Hardwareinformationen zulassen, um die SIM-basierte Lizenzierung zu aktivieren** auswählen.
- b) Wenn Sie die Aktivierungsart Privatsphäre des Benutzers ausgewählt haben und bestimmte Funktionen verwalten möchten, aktivieren Sie die entsprechenden Kontrollkästchen.
- c) Wenn Sie die Aktivierungsarten MDM-Steuerelemente oder Privatsphäre des Benutzers (mit SIM-basierter Lizenzierung) ausgewählt haben und Sie nur beaufsichtigte Geräte aktivieren möchten, wählen Sie **Aktivierung von Geräten ohne Aufsicht nicht zulassen** aus.
- d) Wählen Sie im Abschnitt **Integritätsprüfung der iOS-App** optional eine der folgenden Nachweismethoden aus:
  - **App-Integritätsprüfung bei der Aktivierung der BlackBerry Dynamics-App durchführen:** Verwenden Sie diese Methode, um Prüffragen an Geräte zu senden, wenn sie aktiviert werden, und so die Integrität der geschäftlichen iOS-Apps zu überprüfen.
  - **App-Integritätsprüfung regelmäßig durchführen:** Verwenden Sie diese Methode, um Prüffragen an Geräte zu senden und so die Integrität von geschäftlichen iOS-Apps zu überprüfen.

Um eine iOS-App-Integritätsprüfung durchzuführen, müssen Sie CylancePROTECT in Ihrer UEM-Domäne aktivieren. Weitere Informationen finden Sie unter [Aktivieren von CylancePROTECT Mobile in Ihrer UEM-Domäne](#).

- e) Wählen Sie im Abschnitt **Nachweis eines verwalteten Gerätes** optional eine der folgenden Nachweismethoden aus:
  - **Nachweis eines verwalteten Gerätes bei Geräteaktivierung durchführen:** Verwenden Sie diese Methode, um Prüffragen an Geräte zu senden, wenn sie aktiviert werden, und so die Integrität der Geräteeigenschaften zu überprüfen.
  - **Regelmäßigen Nachweis verwalteter Geräte durchführen:** Verwenden Sie diese Methode, um regelmäßig Prüffragen zu senden, um die Integrität der Geräteeigenschaften zu prüfen.

Um einen Nachweis verwalteter Geräte auf iOS-Geräten durchzuführen, müssen Sie die Funktion aktivieren. Weitere Informationen finden Sie unter [Nachweis für iOS-Geräte konfigurieren](#) in der Dokumentation für Administratoren.

Der Nachweis verwalteter Geräte gilt für die MDM-Steuerelemente- und die Privatsphäre des Benutzers-Aktivierungsarten, jedoch nicht für die Benutzerdatenschutz - Benutzerregistrierung-Aktivierungsart. Wenn Sie die Privatsphäre des Benutzers-Aktivierungsart auswählen, müssen Sie mindestens eine der Verwaltungsoptionen auswählen (z. B. „VPN-Verwaltung zulassen“).

**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.
- b) 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.

- c) Wenn Sie eine der Android Enterprise-Aktivierungsarten ausgewählt haben, wählen Sie die entsprechenden Android Enterprise-Optionen:
- Um die Funktionen von BlackBerry Secure Connect Plus und Knox Platform for Enterprise (für Geräte, die Samsung Knox unterstützen) auf Geräten mit einer entsprechenden Lizenz zu aktivieren, wählen Sie **Bei der Aktivierung von Android Enterprise-Geräten Premium UEM-Funktionen wie z. B. BlackBerry Secure Connect Plus freischalten**.
  - Um die Samsung Knox DualDAR-Verschlüsselung für Geräte zu aktivieren, die diese unterstützen, wählen Sie **Samsung Knox DualDAR Workspace aktivieren**.
  - Um die Google Play-App-Verwaltung im geschäftlichen Bereich zuzulassen, wählen Sie **Google Play zum geschäftlichen Bereich hinzufügen** aus.
  - Um UEM die Sperrung der Aktivierung nach Geräte-ID zu ermöglichen, wählen Sie **Nur genehmigte Geräte-IDs zulassen**. Diese Option wird nur für Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Geräte unterstützt.
  - Um den Netzwerktyp festzulegen, über den Benutzer ein Gerät aktivieren können, wählen Sie in der Dropdown-Liste **Registrierung per QR-Code** ein Netzwerk aus. Diese Option wird nur für Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Geräte unterstützt.
- d) Wählen Sie optional im Abschnitt **Optionen für SafetyNet- oder Play Integrity-Nachweis** eine der folgenden Nachweismethoden aus:
- **SafetyNet- oder Play Integrity-Nachweis für Gerät durchführen:** Verwenden Sie diese Methode, um Abfragen zum Testen der Authentizität und Integrität der Geräte zu senden.
  - **SafetyNet-Nachweis bei Geräteaktivierung durchführen (gilt nur für UEM-Client-Versionen, die Play Integrity nicht unterstützen):** Verwenden Sie diese Methode, um Nachweise zum Testen der Authentizität und Integrität der Geräte zu senden, wenn sie aktiviert werden.
  - **SafetyNet- oder Play Integrity-Nachweis bei der Aktivierung der BlackBerry Dynamics-App durchführen:** Verwenden Sie diese Methode, um Abfragen zum Testen der Authentizität und Integrität der BlackBerry Dynamics-Apps zu senden, wenn sie aktiviert werden.
- e) Wenn UEM Abfragen an Geräte senden soll, wenn diese aktiviert sind, um sicherzustellen, dass die erforderliche Sicherheitspatch-Stufe installiert ist, wählen Sie im Abschnitt **Optionen für Hardware-Nachweis Konformitätsregeln für den Integritätsnachweis während der Aktivierung durchsetzen** aus.

11. Wählen Sie für Windows 10-Geräte eine oder beide Formfaktoroptionen aus.

12. Klicken Sie auf **Hinzufügen**.

**Wenn Sie fertig sind:**

- Legen Sie ggf. eine Rangfolge für die Aktivierungsprofile fest.
- Weisen Sie die Profile Benutzerkonten und -gruppen zu.

# Aktivieren von Android-Geräten

Die Schritte, die Benutzer ausführen, um den BlackBerry UEM Client zu installieren und die Android-Geräte zu aktivieren, hängen von verschiedenen Faktoren ab, z. B. von der Betriebssystemversion von Android, dem Gerätehersteller, der Art und Weise der Verwendung von Google-Diensten in Ihrem Unternehmen, der im Geräteaktivierungsprofil angegebenen Aktivierungsart und von den Präferenzen Ihres Unternehmens. Sie können Anweisungen zur Geräteaktivierung in der Aktivierungs-E-Mail bereitstellen, die Sie an Benutzer senden. Weitere Informationen über das Erstellen von Vorlagen für Aktivierungs-E-Mails finden Sie unter [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).

Android Management-Geräte unterstützen die folgenden Aktivierungsmethoden:

Aktivierungsmethode	Beschreibung
Aktivierung für Android Management-Benutzerdatenschutz	<p>Für Geräte, die mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz aktiviert werden, können Benutzer ein geschäftliches Profil einrichten und einen bereitgestellten QR-Code verwenden, um den UEM Client von Google Play herunterzuladen und das Gerät auf UEM zu aktivieren.</p> <p>Weitere Informationen finden Sie unter <a href="#">Aktivieren eines Android Management-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz</a>.</p>
Aktivierung für Android Management volle Kontrolle und nur geschäftlicher Bereich	<p>Für Geräte, die mit den Aktivierungsarten Geschäftlich und persönlich – vollständige Kontrolle und Nur geschäftlicher Bereich aktiviert werden, muss der Benutzer das Gerät auf die Werkseinstellungen zurücksetzen und einen bereitgestellten QR-Code verwenden, um den UEM Client von Google Play herunterzuladen und das Gerät auf UEM zu aktivieren.</p> <p>Weitere Informationen finden Sie unter <a href="#">Aktivieren eines Android Management-Geräts mit einem verwalteten Google Play-Konto</a>.</p>

Android Enterprise-Geräte unterstützen die folgenden Aktivierungsmethoden:

Aktivierungsmethode	Beschreibung
Installieren des UEM Client aus Google Play.	<p>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 herunterladen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Aktivierung eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz</a>.</p>
Herunterladen der .apk-Datei von UEM Client von der BlackBerry-Download-Website.	<p>Wenn Android-Benutzer bei Geräten, die mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz aktiviert werden, keinen Zugriff auf Google Play haben, können Benutzer die .apk-Datei von UEM Client von der BlackBerry-Download-Website herunterladen. Sie können die Datei auch von BlackBerry herunterladen und an einem Speicherort ablegen, auf den Ihre Benutzer zugreifen können.</p> <p>Informationen zum Erhalt der .apk-Datei der neuesten Version von UEM Client finden Sie in <a href="#">KB 42607</a>.</p>

Aktivierungsmethode	Beschreibung
Verwenden von Domänenanmeldeinformationen für Google während der Geräteeinrichtung.	<p>Wenn BlackBerry UEM mit der Google Workspace- 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.</p> <p>Weitere Informationen finden Sie unter <a href="#">Aktivieren eines Android Enterprise-Geräts, wenn BlackBerry UEM mit einer Google-Domäne verbunden ist</a>.</p>
Scannen eines QR-Codes, der den Speicherort für den UEM Client-Download enthält.	<p>BlackBerry UEM ermöglicht es Ihnen, den Download-Speicherort für den UEM Client als QR-Code abzubilden, den Sie in die Aktivierungs-E-Mail aufnehmen können, die Sie an Benutzer senden. Benutzer, denen Nur geschäftlicher Bereich oder Geschäftlich und persönlich – vollständige Kontrolle zugewiesen ist, können den QR-Code scannen, um den UEM Client herunterzuladen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Aktivieren eines Android Enterprise-Geräts mit einem verwalteten Google Play-Konto</a>.</p>
Android-Zero-Touch-Registrierung oder Samsung Knox Mobile Enrollment.	<p>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.</p> <p>Weitere Informationen finden Sie unter <a href="#">Konfigurieren der Unterstützung für die Android Zero-Touch-Registrierung</a> oder <a href="#">Aktivieren von mehreren Geräten mit Knox Mobile Enrollment</a>.</p>

Bei Android Enterprise-Geräten wird jede Aktivierungsoption 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	AE- Benutzerdatenschutz	Volle AE-Kontrolle			AE 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

Aktivierungsart	AE- Benutzerdatenschutz	Volle AE-Kontrolle			AE Nur geschäftlicher Bereich		
		Google- Domäne	Google Play – verwaltet	Kein Zugriff auf Google	Google- Domäne	Google Play – verwaltet	Kein Zugriff auf Google
Anmeldedaten für die Google-Domäne	Ja	Ja	Nein	Nein	Ja	Nein	Nein
QR-Code scannen	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Android-Zero-Touch-Registrierung/S. Knox Mobile Enrollment	Nein	Ja	Ja	Ja	Ja	Ja	Ja

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

Um Geräte mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) zu aktivieren, senden Sie die folgenden Aktivierungsanweisungen an Gerätebenutzer. Geräte mit dieser Aktivierungsart müssen vor der Aktivierung nicht auf die Werkseinstellungen zurückgesetzt werden.

**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-Nachricht einen QR-Code zur Aktivierung enthält, können Sie damit Ihr Gerät aktivieren. Wenn Sie keinen QR-Code erhalten haben, vergewissern Sie sich, dass Sie die folgenden Informationen haben:

- Ihre geschäftliche E-Mail-Adresse
- Ihr UEM-Benutzername (in der Regel Ihr geschäftlicher Benutzername)
- Ihr UEM-Aktivierungskennwort
- Die 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 mit einer .apk-Datei manuell herunterladen. Informationen zum Erhalt der .apk-Datei der neuesten Version von UEM Client finden Sie in [KB 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
Scannen eines QR-Codes, um das Gerät zu aktivieren.	<ol style="list-style-type: none"> <li>Tippen Sie auf .</li> <li>Damit der UEM Client Fotos und Videos aufnehmen kann, tippen Sie auf <b>Zulassen</b>.</li> <li>Scannen Sie den QR-Code, den Ihr Administrator in der Aktivierungs-E-Mail angegeben hat.</li> </ol>
Manuelles Aktivieren des Geräts.	<ol style="list-style-type: none"> <li>Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf <b>Weiter</b>.</li> <li>Geben Sie Ihr Aktivierungskennwort ein, und tippen Sie auf <b>Mein Gerät aktivieren</b>.</li> <li>Geben Sie ggf. die Serveradresse ein, und tippen Sie auf <b>Weiter</b>.</li> <li>Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein, und tippen Sie auf <b>Weiter</b>.</li> </ol>

- Um UEM Client das Tätigen und Verwalten von Telefonanrufen zu gestatten, tippen Sie auf **Zulassen**.
- Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**. Die Einrichtung des geschäftlichen Profils kann einen Moment dauern.
- Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto an, geben Sie Ihre Google-E-Mail-Adresse und Ihr Kennwort ein.
- Wählen Sie eine Methode zum Entsperren des Bildschirms.
- Tippen Sie auf **Ja**, wenn Sie auf dem Bildschirm **Sicheres Starten** dazu aufgefordert werden, damit zum Starten des Geräts ein Kennwort erforderlich ist.
- Geben Sie ein Gerätekenwort ein, und wiederholen Sie es zur Bestätigung. Tippen Sie auf **OK**.
- Wählen Sie aus, wie Benachrichtigungen angezeigt werden sollen. Tippen Sie auf **Fertig**.
- 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.
- Tippen Sie auf **Registrieren**.
- Wenn Sie die Fingerabdruck-Authentifizierung für die UEM Client- und BlackBerry Dynamics-Apps einrichten möchten, befolgen Sie die Anweisungen auf dem Bildschirm. Tippen Sie andernfalls auf **Abbrechen**.
- Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die UEM-Aktivierung abzuschließen.
- Tippen Sie auf **OK**, wenn Sie dazu aufgefordert werden, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
- Wenn Sie aufgefordert werden, geschäftliche Apps auf Ihrem Gerät zu installieren, befolgen Sie die Anweisungen auf dem Bildschirm.

**Wenn Sie fertig sind:** Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, gehen Sie nach einer der folgenden Methoden vor:

- 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 Google Workspace- 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 [Aktivierung eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz](#).

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
  - Ihr UEM-Benutzername (in der Regel Ihr geschäftlicher Benutzername)
  - Ihr UEM-Aktivierungskennwort
  - Ihre 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 des Geräts mit einem QR Code.	<ol style="list-style-type: none"><li>a. Tippen Sie auf .</li><li>b. Tippen Sie auf <b>Zulassen</b>, damit der UEM Client Fotos und Videos aufnehmen kann.</li><li>c. Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.</li></ol>
Manuelles Aktivieren des Geräts.	<ol style="list-style-type: none"><li>a. Geben Sie Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf <b>Weiter</b>.</li><li>b. Geben Sie Ihr Aktivierungskennwort ein. Tippen Sie auf <b>Mein Gerät aktivieren</b>.</li><li>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 <b>Weiter</b>.</li><li>d. Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein. Tippen Sie auf <b>Weiter</b>.</li></ol>

6. Warten Sie, während die Profile und Einstellungen an Ihr Gerät übertragen werden.

7. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**. Die Einrichtung des geschäftlichen Profils kann einen Moment dauern.
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 Gerätekenntwort 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 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, gehen Sie nach einer der folgenden Methoden vor:

- 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 einem verwalteten Google Play-Konto

Die folgenden Aktivierungsanweisungen gelten für unterstützte Android-Geräte, denen die Aktivierungsart Nur geschäftlicher Bereich (Android Enterprise) oder Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) zugewiesen ist. Informationen zum Aktivieren von Geräten, die mit einem verwalteten Google Play-Konto mit der Aktivierungsart Android Enterprise Geschäftlich und persönlich – Benutzer-Datenschutz verbunden sind, finden Sie unter [Aktivierung eines Android Enterprise-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz](#).

Sie können einen QR Code konfigurieren und aufnehmen, der den Speicherort der Quelldatei der UEM Client-App in der Aktivierungs-E-Mail enthält, die Sie an Benutzer senden. Wenn ein Benutzer den QR Code scannt, wird der UEM Client automatisch heruntergeladen. Um einen QR Code zu konfigurieren und in die Aktivierungs-E-Mail-Nachricht aufzunehmen, müssen Sie das Kontrollkästchen „QR-Codes für Geräteaktivierung zulassen“ auf der Seite „Standardeinstellungen für die Aktivierung“ aktivieren (Einstellungen > Allgemeine Einstellungen > Standardeinstellungen für die Aktivierung). Sie müssen auch das Kontrollkästchen „Zulassen, dass der QR-Code den Speicherort der Quelldatei der UEM Client-App enthält“ aktivieren und den Speicherort der Quelldatei der UEM Client-App angeben. Informationen zum Erhalt der .apk-Datei der neuesten Version von UEM Client finden Sie in [KB 42607](#).

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 seine werksseitigen Standardeinstellungen zurück.
2. Um den QR Code-Leser des Geräts zu öffnen, tippen Sie siebenmal auf den Gerätebildschirm.
3. Um den UEM Client herunterzuladen, scannen Sie den QR Code, den Ihr Administrator in der Aktivierungs-E-Mail angegeben hat.
4. Öffnen Sie den UEM Client.
5. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
6. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**. Die Einrichtung des geschäftlichen Profils kann einen Moment dauern.
7. Wählen Sie eine Methode zum Entsperren des Bildschirms.
8. Tippen Sie auf **Ja**, wenn Sie auf dem Bildschirm **Sicheres Starten** dazu aufgefordert werden, damit zum Starten des Geräts ein Kennwort erforderlich ist.
9. Geben Sie ein Gerätekenwort ein, wiederholen Sie es zur Bestätigung, und tippen Sie dann auf **OK**.
10. Wählen Sie aus, wie 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 **Registrieren**.
13. Wenn Sie die Fingerabdruck-Authentifizierung für die UEM Client- und BlackBerry Dynamics-Apps einrichten möchten, befolgen Sie die Anweisungen auf dem Bildschirm. Tippen Sie andernfalls auf **Abbrechen**.
14. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die UEM-Aktivierung abzuschließen.
15. Tippen Sie auf **OK**, wenn Sie dazu aufgefordert werden, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
16. Wenn Sie aufgefordert werden, geschäftliche Apps auf Ihrem Gerät zu installieren, befolgen Sie die Anweisungen auf dem Bildschirm.

**Wenn Sie fertig sind:** Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, gehen Sie nach einer der folgenden Methoden vor:

- 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

Die folgenden Aktivierungsanweisungen gelten für Geräte, denen die Aktivierungsarten Nur geschäftlicher Bereich (Android Enterprise) und Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) zugewiesen sind und die keinen Zugriff auf Google Play haben. Der Benutzer kann den BlackBerry UEM Client mithilfe einer .apk -Datei der App herunterladen. Sie können einen QR Code konfigurieren und aufnehmen, der den Speicherort der Quelldatei von UEM Client in der Aktivierungs-E-Mail enthält, die Sie an Benutzer senden. Wenn ein Benutzer den QR Code scannt, wird der UEM Client automatisch heruntergeladen.

Um einen QR Code zu konfigurieren und in die Aktivierungs-E-Mail-Nachricht aufzunehmen, müssen Sie das Kontrollkästchen „QR-Codes für Geräteaktivierung zulassen“ auf der Seite „Standardeinstellungen für die Aktivierung“ aktivieren (**Einstellungen > Allgemeine Einstellungen > Standardeinstellungen für die Aktivierung**). Sie müssen auch das Kontrollkästchen „Zulassen, dass der QR-Code den Speicherort der Quelldatei der UEM Client-App enthält“ aktivieren und den Speicherort der Quelldatei der UEM Client-App angeben. Informationen zum Erhalt der .apk-Datei der neuesten Version von UEM Client finden Sie in [KB 42607](#).

Senden Sie die folgenden Aktivierungsanweisungen an 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 eine Aktivierung QR Code von Ihrem Administrator erhalten haben, können Sie damit Ihr Gerät aktivieren. Wenn Sie keinen QR Code erhalten haben, vergewissern Sie sich, dass Sie die folgenden Informationen haben:

- Ihre geschäftliche E-Mail-Adresse
  - Ihr UEM-Benutzername (in der Regel Ihr geschäftlicher Benutzername)
  - Ihr UEM-Aktivierungskennwort
  - Ihre UEM-Serveradresse (falls erforderlich)
1. Wenn Ihnen auf dem zu aktivierenden Gerät der Bildschirm für die Geräteeinrichtung nicht angezeigt wird, setzen Sie das Gerät auf seine werksseitigen Standardeinstellungen zurück.
  2. Um den QR Code-Leser des Geräts zu öffnen, tippen Sie siebenmal auf den Gerätebildschirm.
  3. Um den UEM Client herunterzuladen, scannen Sie den QR Code, den Ihr Administrator in der Aktivierungs-E-Mail angegeben hat.  
Der UEM Client wird automatisch auf das Gerät heruntergeladen.
  4. Öffnen Sie den UEM Client.
  5. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
  6. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren des Geräts mit einem QR Code.	<ol style="list-style-type: none"> <li>a. Tippen Sie im UEM Client auf .</li> <li>b. Damit der UEM Client Fotos und Videos aufnehmen kann, tippen Sie auf <b>Zulassen</b>.</li> </ol>
Manuelles Aktivieren des Geräts.	<ol style="list-style-type: none"> <li>a. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf <b>Weiter</b>.</li> <li>b. Geben Sie Ihr Aktivierungskennwort ein, und tippen Sie auf <b>Mein Gerät aktivieren</b>.</li> <li>c. Geben Sie ggf. die Serveradresse ein, und tippen Sie auf <b>Weiter</b>.</li> <li>d. Geben Sie bei Bedarf Ihren Benutzernamen und Ihr Aktivierungskennwort ein, und tippen Sie auf <b>Weiter</b>.</li> </ol>

7. Tippen Sie auf dem Bildschirm **Profil einrichten** auf **Einrichten**. Die Einrichtung des geschäftlichen Profils kann einen Moment dauern.
8. Wählen Sie eine Methode zum Entsperren des Bildschirms.
9. Tippen Sie auf **Ja**, wenn Sie vom Bildschirm **Sicheres Starten** dazu aufgefordert werden, damit zum Starten des Geräts ein Kennwort erforderlich ist.
10. Geben Sie ein Gerätekenwort ein, und wiederholen Sie es zur Bestätigung. Tippen Sie auf **OK**.
11. Wählen Sie aus, wie Benachrichtigungen angezeigt werden sollen. Tippen Sie auf **Fertig**.

12. 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.
13. Tippen Sie auf dem nächsten Bildschirm auf **Registrieren**.
14. Wenn Sie die Fingerabdruck-Authentifizierung für die UEM Client- und BlackBerry Dynamics-Apps einrichten möchten, befolgen Sie die Anweisungen auf dem Bildschirm. Tippen Sie andernfalls auf **Abbrechen**.
15. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die UEM-Aktivierung abzuschließen.
16. Tippen Sie auf **OK**, wenn Sie dazu aufgefordert werden, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, während die Verbindung hergestellt wird.
17. Wenn Sie aufgefordert werden, geschäftliche Apps auf Ihrem Gerät zu installieren, befolgen Sie die Anweisungen auf dem Bildschirm.
18. Wenn Sie E-Mails auf Ihrem Telefon einrichten möchten, öffnen Sie die E-Mail-App, die Sie für Ihr Unternehmen verwenden sollen, und befolgen Sie die Anweisungen.

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

Sie können in die an Benutzer gesendete Aktivierungs-E-Mail einen QR Code einbetten. Wenn ein Benutzer den QR Code scannt, wird der UEM Client automatisch heruntergeladen. Um einen QR Code zu konfigurieren und in die Aktivierungs-E-Mail-Nachricht aufzunehmen, müssen Sie das Kontrollkästchen „QR-Codes für Geräteaktivierung zulassen“ auf der Seite „Standardeinstellungen für die Aktivierung“ aktivieren (**Einstellungen > Allgemeine Einstellungen > Standardeinstellungen für die Aktivierung**). Verwenden Sie die standardmäßige Android Management-Aktivierungs-E-Mail-Vorlage (oder eine benutzerdefinierte Entsprechung).

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. Gehen Sie auf Ihrem Gerät zu **Einstellungen > Google-Dienste und -Voreinstellungen**.
2. Tippen Sie auf **Einrichtung und Wiederherstellung**.
3. Tippen Sie auf **Geschäftliches Profil einrichten**.
4. Tippen Sie auf **Weiter**.
5. Tippen Sie im Dialogfeld **Geräterichtlinie erlauben, Bilder und Videos aufzunehmen** auf **Nur dieses Mal**.
6. Scannen Sie den QR-Code, den Sie von Ihrem Administrator erhalten haben.
7. Tippen Sie auf **Zustimmen**.
8. Tippen Sie auf **Weiter**.
9. Je nachdem, wie Ihr Administrator die Aktivierung konfiguriert hat, werden Sie möglicherweise aufgefordert, eine Sperre für Ihr Gerät oder den geschäftlichen Bereich festzulegen.
10. Tippen Sie auf dem Bildschirm **Ihre geschäftliche Prüfliste** unter **Installieren von geschäftlichen Apps** auf **Installieren**.
11. Tippen Sie nach der Installation des UEM Client auf **Fertig**.
12. Tippen Sie auf **BlackBerry UEM einrichten**.
13. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf **Zustimmen**.

Ihr Gerät wird die Einrichtung Ihres geschäftlichen Profils abschließen.

**Wenn Sie fertig sind:** Wenn Sie Ihr Gerät deaktivieren und aus UEM entfernen möchten, können Sie dies über den UEM Client tun.

# Aktivieren eines Android Management-Geräts mit einem verwalteten Google Play-Konto

Die folgenden Aktivierungsanweisungen gelten für Android-Geräte, denen die Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle (Android Management) oder Nur geschäftlicher Bereich (Android Management) zugewiesen ist. Informationen zum Aktivieren von Geräten, die mit einem verwalteten Google Play-Konto mit der Aktivierungsart Android Management Geschäftlich und persönlich – Benutzer-Datenschutz verbunden sind, finden Sie unter [Aktivieren eines Android Management-Geräts mit der Aktivierungsart Geschäftlich und persönlich – Benutzer-Datenschutz](#).

Sie können in die an Benutzer gesendete Aktivierungs-E-Mail einen QR Code einbetten. Wenn ein Benutzer den QR Code scannt, wird der UEM Client automatisch heruntergeladen. Um einen QR Code zu konfigurieren und in die Aktivierungs-E-Mail-Nachricht aufzunehmen, müssen Sie das Kontrollkästchen „QR-Codes für Geräteaktivierung zulassen“ auf der Seite „Standardeinstellungen für die Aktivierung“ aktivieren (**Einstellungen > Allgemeine Einstellungen > Standardeinstellungen für die Aktivierung**). Verwenden Sie die standardmäßige Android Management-Aktivierungs-E-Mail-Vorlage (oder eine benutzerdefinierte Entsprechung).

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 seine werkseitigen Standardeinstellungen zurück.
2. Um den QR Code-Leser des Geräts zu öffnen, tippen Sie siebenmal auf den Gerätebildschirm.
3. Um den UEM Client herunterzuladen, scannen Sie den QR Code, den Ihr Administrator in der Aktivierungs-E-Mail angegeben hat.  
Der UEM Client wird automatisch heruntergeladen.
4. Öffnen Sie den UEM Client.
5. Lesen Sie die Lizenzvereinbarung, und tippen Sie auf das Kontrollkästchen **Ich nehme die Lizenzvereinbarung an**.
6. Tippen Sie auf dem Bildschirm **Profil einrichten auf Einrichten**. Die Einrichtung des geschäftlichen Profils kann einen Moment dauern.
7. Wählen Sie eine Methode zum Entsperren des Bildschirms.
8. Tippen Sie auf **Ja**, wenn Sie auf dem Bildschirm **Sicheres Starten** dazu aufgefordert werden, damit zum Starten des Geräts ein Kennwort erforderlich ist.
9. Geben Sie ein Gerätekenntwort ein, wiederholen Sie es zur Bestätigung, und tippen Sie dann auf **OK**.
10. Wählen Sie aus, wie Benachrichtigungen angezeigt werden sollen, und tippen Sie dann 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 **Registrieren**.
13. Wenn Sie die Fingerabdruck-Authentifizierung für die UEM Client- und BlackBerry Dynamics-Apps einrichten möchten, befolgen Sie die Anweisungen auf dem Bildschirm. Tippen Sie andernfalls auf **Abbrechen**.
14. Wenn Sie von Ihrem Gerät abgemeldet sind, entsperren Sie Ihr Gerät, um die BlackBerry UEM-Aktivierung abzuschließen.
15. Tippen Sie auf **OK**, wenn Sie dazu aufgefordert werden, um die Verbindung mit BlackBerry Secure Connect Plus zuzulassen, und warten Sie, bis die Verbindung hergestellt wurde.
16. Wenn Sie aufgefordert werden, geschäftliche Apps auf Ihrem Gerät zu installieren, befolgen Sie die Anweisungen auf dem Bildschirm.

**Wenn Sie fertig sind:** Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, gehen Sie nach einer der folgenden Methoden vor:

- 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 von iOS-Geräten

Die Schritte, die Benutzer befolgen, um die BlackBerry UEM Client iOS-Geräte zu installieren und die iPadOS-Geräte zu aktivieren, hängen von der Betriebssystemversion des Geräts und davon ab, ob die Aktivierungsart MDM-Steuer-elemente enthält. Sie können Anweisungen zur Geräteaktivierung in der Aktivierungs-E-Mail bereitstellen, die Sie an Benutzer senden. Weitere Informationen über das Erstellen von Vorlagen für Aktivierungs-E-Mails finden Sie unter [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).

## Aktivierung eines iOS- oder iPadOS-Geräts mit der Aktivierungsart MDM-Steuer-elemente

Um Geräte mit der Aktivierungsart MDM-Steuer-elemente oder Privatsphäre des Benutzers mit aktivierten MDM-Optionen zu aktivieren, senden Sie die folgenden Aktivierungsanweisungen an Gerätebenutzer.

Während der Aktivierung müssen Benutzer den BlackBerry UEM Client verlassen, um das MDM-Profil manuell zu installieren.

**Bevor Sie beginnen:** Wenn der Sperrmodus auf Ihrem Gerät aktiviert ist (iOS und iPadOS 16 oder höher), müssen Sie ihn für die Aktivierung des Geräts deaktivieren. Der Sperrmodus verhindert die Installation von Konfigurationsprofilen, die für die Aktivierung erforderlich sind. Bei Bedarf können Sie den Sperrmodus nach der Aktivierung wieder aktivieren.

1. Installieren Sie den UEM Client aus dem App Store auf dem Gerät.
2. Öffnen Sie den UEM Client, und stimmen Sie der Lizenzvereinbarung zu.
3. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Scannen Sie einen QR Code, um das Gerät zu aktivieren.	<ol style="list-style-type: none"><li>a. Tippen Sie auf .</li><li>b. Damit der UEM Client Fotos und Videos aufnehmen kann, tippen Sie auf <b>Zulassen</b>.</li><li>c. Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.</li></ol>
Manuelles Aktivieren des Geräts.	<ol style="list-style-type: none"><li>a. Geben Sie Ihre geschäftliche E-Mail-Adresse und Ihr Aktivierungskennwort ein.</li><li>b. Geben Sie ggf. die Serveradresse ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service.</li><li>c. Tippen Sie auf <b>Weiter</b>.</li></ol>

4. Tippen Sie auf **Zulassen**, damit UEM Client Ihnen Benachrichtigungen senden kann. Wenn Sie **Nicht zulassen** wählen, wird die Aktivierung des Geräts verhindert.
5. Wenn Sie aufgefordert werden, ein Konfigurationsprofil zu installieren, tippen Sie auf **OK**.
6. Wenn Sie zum Herunterladen des Konfigurationsprofils aufgefordert werden, tippen Sie auf **Zulassen**.
7. Nachdem der Download abgeschlossen ist, öffnen Sie **Einstellungen**.
8. Tippen Sie auf **Allgemein**, und navigieren Sie zu **VPN- und Geräteverwaltung**.
9. Tippen Sie zum Installieren des Profils auf **BlackBerry UEM-Profil**, und befolgen Sie die Anweisungen auf dem Bildschirm.

10. Wenn die Installation abgeschlossen ist, kehren Sie zum Abschluss der Aktivierung zum UEM Client zurück.

11. Wenn Sie aufgefordert werden, geschäftliche Apps auf Ihrem Gerät zu installieren, befolgen Sie die Anweisungen auf dem Bildschirm.

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

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

## Aktivieren eines iOS- oder iPadOS-Geräts mit Apple-Benutzerregistrierung

Die Apple-Benutzerregistrierung wird auf Geräten unterstützt, auf denen die unterstützten Versionen von iOS und iPadOS ausgeführt werden. Um Geräte mit Apple-Benutzeranmeldung zu aktivieren, senden Sie die folgenden Aktivierungsanweisungen an Gerätebenutzer.

### Bevor Sie beginnen:

- Stellen Sie sicher, dass Sie eine Aktivierungs-E-Mail mit dem QR Code für die Apple-Benutzerregistrierung erhalten haben. Wenn Sie die E-Mail nicht erhalten haben, wenden Sie sich an einen Administrator.
  - Wenn das Gerät bereits mit BlackBerry UEM aktiviert ist, müssen Sie das Gerät deaktivieren.
  - Deinstallieren Sie den BlackBerry UEM Client.
  - Sie müssen über ein Apple ID-Konto verfügen, das über Ihr Unternehmen verwaltet wird.
  - Das Gerät darf kein überwachtes Gerät sein. Wenn Ihr Gerät überwacht wird, wird dies in den App-Einstellungen in der Nähe Ihrer Apple ID angezeigt.
  - Wenn der Sperrmodus auf Ihrem Gerät aktiviert ist (iOS und iPadOS 16 oder höher), müssen Sie ihn deaktivieren, um das Gerät zu aktivieren. Der Sperrmodus verhindert die Installation von Konfigurationsprofilen, die für die Aktivierung erforderlich sind. Bei Bedarf können Sie den Sperrmodus nach der Aktivierung wieder aktivieren.
1. Öffnen Sie die Aktivierungs-E-Mail mit dem QR Code für die Apple-Benutzerregistrierung. Wenn der QR Code abgelaufen ist, fordern Sie einen neuen Aktivierungscode von BlackBerry UEM Self-Service an, oder wenden Sie sich an Ihren Administrator.
  2. Öffnen Sie auf Ihrem Gerät die Kamera-App, und scannen Sie den QR-Code in der Aktivierungs-E-Mail. Wenn Sie dazu aufgefordert werden, tippen Sie auf die Benachrichtigung, um die URL in Safari zu öffnen.
  3. Wenn Sie zum Herunterladen des UEM-Konfigurationsprofils aufgefordert werden, tippen Sie auf **Zulassen**.
  4. Nachdem der Download abgeschlossen ist, tippen Sie auf **Schließen**.
  5. Gehen Sie zu **Einstellungen > Allgemein > Profil**.
  6. Tippen Sie auf **UEM-Profil**.
  7. Tippen Sie auf dem Benutzerregistrierungsbildschirm auf **Mein iPhone registrieren** oder **Mein iPad registrieren**.
  8. Geben Sie Ihre Kennung ein.
  9. Melden Sie sich mit Ihren verwalteten Apple ID-Anmeldeinformationen bei der Apple ID an.
  10. Wenn Ihr Administrator Ihnen den UEM Client zugewiesen hat, tippen Sie bei Aufforderung auf **Installieren**, oder öffnen Sie „Geschäftliche Apps“.
  11. Um den UEM Client einzurichten, öffnen Sie ihn und akzeptieren Sie die Lizenzvereinbarung. Folgen Sie den Anweisungen auf dem Bildschirm, um den Aktivierungsprozess abzuschließen.

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

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

# Aktivieren eines macOS- oder Apple TV-Geräts mit BlackBerry UEM Self-Service

Benutzer aktivieren macOS- und Apple TV-Geräte mithilfe von BlackBerry UEM Self-Service. Weitere Informationen und Anweisungen finden Sie im [Benutzerhandbuch zum UEM Self-Service](#).

# Aktivieren eines Windows 10-Tablets oder -Computers

Um Windows 10-Geräte zu aktivieren, senden Sie die folgenden Aktivierungsanweisungen an Gerätebenutzer. Beachten Sie, dass Windows 10-Geräte mit der Aktivierungsart MDM-Steuer-elemente nicht von Microsoft System Center Configuration Manager verwaltet werden können.

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

**Bevor Sie beginnen:** Stellen Sie sicher, dass Sie eine Aktivierungs-E-Mail mit einer Zertifikatsserveradresse erhalten haben. Wenn Sie die E-Mail nicht erhalten haben, wenden Sie sich an Ihren Administrator.

1. Geben Sie im Browser Ihres Geräts die Zertifikatsserveradresse ein.
2. Klicken Sie auf **Speichern**.
3. Klicken Sie in der Download-Benachrichtigung für das Zertifikat auf **Öffnen**.
4. Klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Zertifikat installieren**.
6. Klicken Sie auf die Option **Aktueller Benutzer** und dann auf **Weiter**.
7. Wählen Sie die Option **Alle Zertifikate im folgenden Speicher ablegen**, und klicken Sie auf **Durchsuchen**.
8. Wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen** aus, und klicken Sie auf **OK**.
9. Klicken Sie auf **Weiter > Fertigstellen > OK > OK**.
10. Klicken Sie auf die Schaltfläche **Start**.
11. Führen Sie einen der folgenden Schritte aus:

Geräte-Betriebssystemversion	Schritte
Windows 10 Version 1607 oder höher	<ol style="list-style-type: none"><li>a. Tippen Sie auf <b>Einstellungen &gt; Konten &gt; Geschäftlich oder Schule</b>.</li><li>b. Tippen Sie auf <b>Nur bei der Geräteverwaltung anmelden</b>.</li></ol>
Windows 10-Version vor 1607	<ol style="list-style-type: none"><li>a. Tippen Sie auf <b>Einstellungen &gt; Konten &gt; Geschäftlicher Zugriff</b>.</li><li>b. Tippen Sie auf <b>Verbinden</b>.</li></ol>

12. Geben Sie in das Feld **E-Mail-Adresse** Ihre E-Mail-Adresse ein, und tippen Sie auf **Fortfahren**.
13. Wenn Sie dazu aufgefordert werden, geben Sie im Feld **Server** den Servernamen ein, und tippen Sie auf **Fortfahren**. Sie finden Ihre Serveradresse in der Aktivierungs-E-Mail, die Sie von Ihrem Administrator erhalten haben, oder im BlackBerry UEM Self-Service, wenn Sie Ihr Aktivierungskennwort einstellen.
14. Geben Sie im Feld **Aktivierungskennwort** Ihr Aktivierungskennwort ein, und tippen Sie auf **Weiter**. Sie finden Ihr Aktivierungskennwort in der Aktivierungs-E-Mail, die Sie von Ihrem Administrator erhalten haben, oder Sie können Ihr eigenes Kennwort mit dem UEM Self-Service einrichten.
15. Tippen Sie auf **Fertig**.

**Wenn Sie fertig sind:**

- Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:
  - Klicken Sie auf Ihrem Gerät auf **„Einstellungen > Konten > Geschäftlich oder Schule“** (oder **„Geschäftlicher Zugriff“**), und überprüfen Sie, ob Ihr Gerät mit UEM verbunden ist.
  - Überprüfen Sie im UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.
- Wenn Ihr Administrator dies fordert, fügen Sie Ihr geschäftliches Konto zu **„Von anderen Apps verwendete Konten“** hinzu, damit Sie auf die erforderlichen Online-Apps zugreifen können.

- Bei Windows 10 Version 1607 oder höher klicken Sie auf **„Einstellungen“** > **„Konten“** > **„Geschäftlich oder Schule“** > „Verbinden“. Geben Sie Ihre geschäftliche E-Mail-Adresse und das Kennwort ein.
- Bei einer Windows 10 Version vor 1607 klicken Sie auf **„Einstellungen“** > **„Konten“** > **„Ihre E-Mail-Adresse und Konten“**. Klicken Sie unter „Von anderen Apps verwendete Konten“ auf „Geschäftliches oder Schulkonto hinzufügen“, und geben Sie Ihre geschäftliche E-Mail-Adresse und das Kennwort ein.

# Konfigurieren der Unterstützung für die Android Zero-Touch-Registrierung

Sie können Android-Zero-Touch-Registrierung in BlackBerry UEM verwenden, um eine große Anzahl von Android Enterprise-Geräten gleichzeitig bereitzustellen. Die Geräte müssen Zero-Touch-Registrierung unterstützen.

Wenn Ihr Unternehmen die unterstützten Geräte von einem autorisierten Enterprise-Händler kauft, wird dort ein Konto für die Zero-Touch-Registrierung erstellt und die Geräte dem Konto hinzugefügt. Wenn ein Benutzer eines dieser Geräte zum ersten Mal einrichtet oder ein Gerät auf die Werkseinstellungen zurücksetzt, lädt das Gerät automatisch den BlackBerry UEM Client herunter und startet den UEM-Aktivierungsvorgang.

Beachten Sie, dass wenn der Benutzer das Gerät neu startet, bevor die Aktivierung abgeschlossen ist, die Aktivierung abbricht oder den Akku entlädt, bevor die Aktivierung abgeschlossen ist, wird das Gerät automatisch auf seine Werkseinstellungen zurückgesetzt, und der Aktivierungsvorgang wird neu gestartet.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration**.
2. Klicken Sie auf **Android Enterprise**.
3. Klicken Sie auf **Zero-Touch-Konsole starten**.
4. Wenn Sie zum ersten Mal eine Verbindung zu Android Zero Touch mit UEM hergestellt haben, klicken Sie auf **Weiter**, und melden Sie sich mit der Adresse bei Google an, die dem Zero-Touch-Konto Ihres Unternehmens zugeordnet ist.
5. Erstellen oder verwalten Sie Registrierungskonfigurationen, und weisen Sie sie den Geräten zu.  
Sie können auch das Android-Zero-Touch-Portal verwenden, um die Registrierungskonfigurationen zu verwalten.

## Wenn Sie fertig sind:

- Prüfen Sie in UEM, ob die entsprechenden Profile und IT-Richtlinien den Benutzern zugewiesen wurden. Um die Zero-Touch-Registrierung zu verwenden, müssen Sie ein Aktivierungsprofil mit aktivierter Aktivierungsart „Geschäftlich und persönlich – volle Kontrolle (Android Enterprise)“ oder „Nur geschäftlicher Bereich (Android Enterprise)“ zuweisen.
- Verteilen Sie die Geräte an die Benutzer.

# Aktivieren von mehreren Geräten mit Knox Mobile Enrollment

Sie können Samsung Knox Mobile Enrollment verwenden, um eine große Anzahl von Samsung Knox-Geräten gleichzeitig bereitzustellen. Ihr Unternehmen kauft Geräte von einem autorisierten Händler oder von einem Vertriebspartner, der die IMEI der Geräte direkt mit Samsung teilt, damit das Gerät Knox Mobile Enrollment verwenden kann. Wenn ein Benutzer eines dieser Geräte zum ersten Mal einrichtet oder ein Gerät auf die Werkseinstellungen zurücksetzt, lädt das Gerät automatisch den BlackBerry UEM Client herunter und startet den BlackBerry UEM-Aktivierungsvorgang.

Beachten Sie, dass wenn der Benutzer das Gerät neu startet, bevor die Aktivierung abgeschlossen ist, die Aktivierung abbricht, oder wenn er vor der Aktivierung den Akku entlädt, wird das Gerät automatisch auf die Werkseinstellungen zurückgesetzt, und der Aktivierungsvorgang wird neu gestartet.

**Hinweis:** Knox Mobile Enrollment unterstützt keine administratorbasierte Registrierung auf Geräten, auf denen Android 11 oder höher ausgeführt wird. Weitere Informationen finden Sie in den [Versionshinweisen zu Knox Mobile Enrollment 1.36](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Einstellungen > Externe Integration > KNOX Mobile Enrollment**.
2. Laden Sie die UEM JSON-Datei herunter.
3. Folgen Sie den Schritten auf dem Bildschirm.

**Wenn Sie fertig sind:** Vergleichen Sie nach Abschluss der Aktivierung mit der JSON-Datei, die Sie heruntergeladen haben, den Eintrag im Abschnitt CFPrint mit dem Eintrag, den Sie bei der Konfiguration von Knox Mobile Enrollment hinzugefügt haben. Wenn die Einträge unterschiedlich sind, kopieren Sie auf der Seite Knox Mobile Enrollment im Feld **Benutzerdefinierte JSON-Daten** den gesamten Text aus der .json-Datei.

# Aktivieren von beim DEP registrierten iOS-Geräten

Sie können iOS- und iPadOS-Geräte beim Programm zur Geräteregistrierung (DEP) von Apple registrieren und diesen mit der BlackBerry UEM-Verwaltungskonsolle Registrierungskonfigurationen zuweisen. Registrierungskonfigurationen enthalten zusätzliche Regeln, die Geräten bei der MDM-Registrierung zugewiesen werden.

Sie können ein Apple Business Manager-Konto für die Synchronisation von UEM mit DEP verwenden. Apple Business Manager ist ein Web-basiertes Portal, das es Ihnen ermöglicht, iOS-Geräte in DEP zu registrieren und zu verwalten. Außerdem ist darin die Verwaltung von Apple-VPP-Konten möglich. Wenn Ihr Unternehmen DEP oder VPP verwendet, können Sie auf Apple Business Manager aktualisieren.

Um Geräte zu aktivieren, die in DEP registriert sind, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Registrieren von iOS-Geräten in DEP und Zuweisen eines BlackBerry UEM-Servers.
2	DEP-Registrierungskonfiguration hinzuzufügen.
3	Informationen zum Hinzufügen von BlackBerry UEM Client zur App-Liste und wie man es Benutzerkonten oder Benutzergruppen zuweist, finden Sie unter <a href="#">Hinzufügen einer iOS-App zur App-Liste</a> .
4	Wenn Sie das standardmäßige Aktivierungsprofil nicht verwenden möchten, <a href="#">erstellen Sie ein Aktivierungsprofil</a> , und weisen Sie es DEP-Geräten zu (Benutzer > Apple DEP-Geräte).
5	Wählen Sie, wie Benutzer ihre Geräte aktivieren sollen: <ul style="list-style-type: none"><li>• <a href="#">Senden einer Aktivierungs-E-Mail an mehrere Benutzer</a> oder <a href="#">Senden einer Aktivierungs-E-Mail an einen bestimmten Benutzer</a> mithilfe der Apple-DEP-E-Mail-Vorlage.</li><li>• Wenn Sie UEM mit Ihrem Unternehmensverzeichnis verbunden haben, können Benutzer ihre Benutzernamen und Kennwörter für das Unternehmensverzeichnis verwenden. Benutzer müssen ihren Benutzernamen im Format <code>domäne\benutzername</code> eingeben. (Die Anmeldeinformationen stimmen mit den Variablen Ihres Unternehmens für Domänen- und Benutzername überein („%UserDomain%%UserName%“).</li><li>• <a href="#">Einem iOS-Gerät einen Benutzer zuweisen</a> ist möglich. Wenn Sie dem Gerät in UEM einen Benutzer zuweisen, wird der Benutzer während der Geräteaktivierung nicht zur Eingabe eines Benutzernamens oder Kennworts aufgefordert.</li></ul>
6	Verteilen Sie Geräte an die Benutzer, und fordern Sie sie zum Abschluss der Aktivierung auf. Nach Abschluss der Aktivierung müssen Benutzer den UEM Client installieren und öffnen.

# Registrieren von iOS-Geräten in DEP und Zuweisen eines BlackBerry UEM-Servers

Zum Registrieren von iOS-Geräten im Programm zur Geräteregistrierung (DEP) von Apple müssen Sie die Geräteseriennummern im Apple Business Manager- oder DEP-Portal eingeben und die Geräte dem BlackBerry UEM-Server zuweisen. Um die Seriennummern einzugeben, können Sie jede einzelne Nummer eintippen, die Bestellnummer auswählen, die Apple den Geräten beim Kauf zugewiesen hat, oder eine .csv-Datei hochladen, die die Seriennummern enthält.

**Bevor Sie beginnen:** [Konfigurieren von BlackBerry UEM für DEP](#).

1. Melden Sie sich beim Apple Business Manager oder beim DEP-Portal an.
2. Klicken Sie im Abschnitt **Programm zur Geräteregistrierung** auf **Gerät verwalten**.
3. Befolgen Sie die Schritte auf dem Bildschirm, um Seriennummern von Geräten einzugeben.
4. Weisen Sie die Seriennummern dem UEM-Server zu.

**Wenn Sie fertig sind:** [DEP-Registrierungskonfiguration hinzuzufügen](#).

## DEP-Registrierungskonfiguration hinzuzufügen

Eine Registrierungskonfiguration legt fest, wie in DEP registrierte Geräte eingerichtet werden, wenn sie mit BlackBerry UEM aktiviert werden. Sie können nach Bedarf beliebig viele Registrierungskonfigurationen erstellen.

**Bevor Sie beginnen:** [Registrieren von iOS-Geräten in DEP und Zuweisen eines BlackBerry UEM-Servers](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf den Namen des DEP-Kontos.
3. Klicken Sie im Abschnitt **DEP-Anmeldungskonfigurationen** auf **+**.
4. Geben Sie einen Namen für die Konfiguration ein.
5. Wenn UEM die Registrierungskonfiguration automatisch Geräten zuweisen soll, sobald DEP-Geräte mit UEM synchronisiert werden, aktivieren Sie das Kontrollkästchen **Alle neuen Geräte automatisch dieser Konfiguration zuweisen**.

UEM führt die Synchronisierung mit Apple DEP täglich und jedes Mal, wenn Sie die Seite mit den Apple DEP-Geräten aufrufen, durch. Sie können nur eine Registrierungskonfiguration neuen DEP-Geräten automatisch zuweisen. Wenn Sie zuvor eine Registrierungskonfiguration mit dieser Einstellung erstellt haben, wird die Einstellung automatisch aus der vorherigen Konfiguration entfernt und der neuen Konfiguration hinzugefügt. Wenn Sie zuvor eine Registrierungskonfiguration mit dieser Einstellung erstellt haben und diese auf Geräte angewendet wurde, weist UEM die neue Registrierungskonfiguration nicht zu.

6. Geben Sie optional einen Abteilungsnamen und eine Supporttelefonnummer ein, die während der Einrichtung auf Geräten angezeigt werden sollen.
7. Wählen Sie im Abschnitt **Gerätekonfiguration** eine der folgenden Optionen aus:
  - **Kopplung zulassen:** Benutzer können das Gerät mit einem Computer koppeln.
  - **Erforderlich:** Benutzer werden nicht aufgefordert, die Registrierungskonfiguration anzunehmen.
  - **Entfernen des MDM-Profiles zulassen:** Benutzer können Geräte deaktivieren.
  - **Warten, bis das Gerät konfiguriert wurde:** Benutzer können die Geräteeinrichtung nicht abbrechen, bis der Aktivierungsvorgang abgeschlossen ist.
8. Wählen Sie im Abschnitt **Bei der Einrichtung überspringen** die Elemente aus, die nicht in der Geräteeinrichtung enthalten sein sollen:

<b>Option</b>	<b>Auswirkungen bei Auswahl</b>
Kennung	Benutzer werden nicht aufgefordert, eine Geräteerkennung zu erstellen.
Standortdienste	Standortdienste sind auf dem Gerät deaktiviert.
Wiederherstellen	Benutzer können keine Daten aus einer Sicherungsdatei wiederherstellen.
Verschieben von Android	Daten können von einem Android-Gerät nicht wiederhergestellt werden.
Apple-ID	Benutzer können sich nicht bei Apple-ID und iCloud anmelden.
Geschäftsbedingungen	Benutzer sehen die Geschäftsbedingungen von iOS nicht.
Siri	Siri ist auf Geräten deaktiviert.
Diagnostics	Diagnoseinformationen werden während der Einrichtung nicht automatisch vom Gerät gesendet.
Biometrisch	Benutzer können Touch ID nicht einrichten.
Zahlung	Benutzer können Apple Pay nicht einrichten.
Zoom	Benutzer können Zoom nicht einrichten.
Home-Taste einrichten	Benutzer können den Klick auf die Home-Taste nicht anpassen.
Bildschirmzeit	Die Option zum Einrichten der Bildschirmzeit wird während der DEP-Registrierung übersprungen.
Softwareupdate	Benutzern wird der Bildschirm für obligatorische Softwareupdates auf dem Gerät nicht angezeigt.
iMessage und FaceTime	Benutzer sehen den Bildschirm für iMessage und FaceTime auf dem Gerät nicht.
Anzeigename	Benutzern wird der Bildschirm für den Anzeigenamen auf dem Gerät nicht angezeigt.
Datenschutz	Benutzern wird der Bildschirm für den Datenschutz auf dem Gerät nicht angezeigt.
Onboarding	Benutzern wird der Informationsbildschirm für das Onboarding auf dem Gerät nicht angezeigt.
Watch-Migration	Benutzern wird der Informationsbildschirm für die Watch-Migration auf dem Gerät nicht angezeigt.
SIM-Setup	Benutzern wird der Bildschirm für das Einrichten eines Mobilfunkvertrags auf dem Gerät nicht angezeigt.

Option	Auswirkungen bei Auswahl
Migration von Gerät zu Gerät	Benutzern wird der Informationsbildschirm für die Migration von Gerät zu Gerät auf dem Gerät nicht angezeigt.

9. Klicken Sie auf **Speichern**. Wenn Sie das Kontrollkästchen **Alle neuen Geräte automatisch dieser Konfiguration zuweisen** ausgewählt haben, klicken Sie auf **Ja**.

**Wenn Sie fertig sind:**

- Wenn Sie das Kontrollkästchen **Alle neuen Geräte automatisch dieser Konfiguration zuweisen** nicht aktiviert haben, müssen Sie den Geräten die entsprechende Registrierungskonfiguration zuweisen. Wählen Sie unter **Benutzer > Apple DEP-Geräte** die Geräte aus, die mit demselben DEP-Konto registriert sind, und klicken Sie auf . Wählen Sie die Registrierungskonfiguration aus, und weisen Sie sie zu.
- Wenn Sie das standardmäßige Aktivierungsprofil nicht verwenden möchten, [erstellen Sie ein Aktivierungsprofil](#), und weisen Sie es in Apple DEP registrierten Geräten zu. Wählen Sie unter **Benutzer > Apple DEP-Geräte** die Geräte aus, die mit demselben DEP-Konto registriert sind, und klicken Sie auf . Wählen Sie das Profil aus, und weisen Sie es zu.
- Während der Geräteaktivierung werden Benutzer möglicherweise zur Eingabe eines Benutzernamens und Kennworts aufgefordert. Wählen Sie, wie Benutzer ihre Geräte aktivieren sollen:
  - [Senden einer Aktivierungs-E-Mail an mehrere Benutzer](#) oder [Senden einer Aktivierungs-E-Mail an einen bestimmten Benutzer](#) mithilfe der Apple-DEP-E-Mail-Vorlage.
  - Wenn Sie UEM mit Ihrem Unternehmensverzeichnis verbunden haben, können Benutzer ihre Benutzernamen und Kennwörter für das Unternehmensverzeichnis verwenden. Benutzer müssen ihren Benutzernamen im Format domäne\benutzername eingeben. (Die Anmeldeinformationen stimmen mit den Variablen Ihres Unternehmens für Domänen- und Benutzername überein („%UserDomain%\%UserName%“).
  - [Einem iOS-Gerät einen Benutzer zuweisen](#) ist möglich. Wenn Sie dem Gerät in UEM einen Benutzer zuweisen, wird der Benutzer während der Geräteaktivierung nicht zur Eingabe eines Benutzernamens oder Kennworts aufgefordert.
- Verteilen Sie Geräte an die Benutzer, und fordern Sie sie zum Abschluss der Aktivierung auf. Nach Abschluss der Aktivierung müssen Benutzer den BlackBerry UEM Client installieren und öffnen.

## Einem iOS-Gerät einen Benutzer zuweisen

Sie können einen Benutzer direkt einem in Apple DEP registrierten Gerät zuweisen, bevor das Gerät aktiviert wird. Wenn Sie dem Gerät einen Benutzer direkt zuweisen, wird er während der Geräteaktivierung nicht zur Eingabe eines Benutzernamens oder Kennworts aufgefordert.

1. Klicken Sie in der Menüleiste auf **Benutzer > Apple DEP-Geräte**.
2. Klicken Sie in der Spalte **Benutzerzuordnung** für das Gerät, das Sie zuweisen möchten, auf **Auswählen**.
3. Im Suchfeld **Benutzer auswählen** können Sie nach dem Benutzer suchen, der dem Gerät zugewiesen werden soll.
4. Klicken Sie im Suchergebnis auf das Benutzerkonto.
5. Klicken Sie auf **Speichern**.

**Wenn Sie fertig sind:**

- Um den Eigentümer eines aktivierten Geräts anzuzeigen, klicken Sie in der Spalte **Benutzerzuordnung** auf den Benutzernamen-Link.

- Um einen Benutzer von einem iOS-Gerät zu entfernen, klicken Sie in der Spalte **Benutzerzuordnung** auf den Benutzernamen-Link des Geräts, von dem Sie den Benutzer entfernen möchten. Klicken Sie auf **Zuweisung aufheben**.

# Aktivieren von iOS-Geräten mit Apple Configurator 2

Wenn Sie BlackBerry UEM lokal verwenden, können Sie mithilfe von Apple Configurator 2 iOS- und iPadOS-Geräte für die Aktivierung vorbereiten. Benutzer können die vorbereiteten Geräte aktivieren, ohne den BlackBerry UEM Client verwenden zu müssen. Benutzer brauchen nur ihren Benutzernamen und ihr Aktivierungskennwort.

Apple Configurator wird nicht von UEM Cloud unterstützt.

**Hinweis:** Für bestimmte UEM-Funktionen müssen Sie Benutzern UEM Client zuweisen. Benutzer müssen den UEM Client starten, nachdem sie das Gerät aktivieren. Weitere Informationen finden Sie in [KB 39313](#).

Um iOS-Geräte mit Apple Configurator 2 zu aktivieren, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Fügen Sie optional den UEM Client zur App-Liste hinzu, und weisen Sie ihn Benutzergruppen oder Benutzerkonten zu. Siehe <a href="#">Hinzufügen einer iOS-App zur App-Liste</a> .
2	Hinzufügen von BlackBerry UEM-Serverinformationen zu Apple Configurator 2.
3	Vorbereiten von iOS-Geräten mit Apple Configurator 2.
4	Erstellen Sie ein Aktivierungsprofil, und weisen Sie es einem Benutzerkonto oder einer Benutzergruppe zu.
5	Senden einer Aktivierungs-E-Mail an mehrere Benutzer oder Senden einer Aktivierungs-E-Mail an einen bestimmten Benutzer.
6	Verteilen Sie Geräte an die Benutzer, und fordern Sie sie zum Abschluss der Aktivierung auf. Um ein Konformitätsprofil zu erzwingen, müssen die Benutzer nach Abschluss der Aktivierung den UEM Client installieren und öffnen.

## Hinzufügen von BlackBerry UEM-Serverinformationen zu Apple Configurator 2

**Bevor Sie beginnen:** Laden Sie die aktuelle Version des Apple Configurator 2 von Apple herunter, und installieren Sie ihn.

1. Wählen Sie im Apple Configurator 2-Menü **Einstellungen > Server** aus.
2. Klicken Sie auf **+ > Weiter**.
3. Geben Sie im Feld **Name** einen Namen für den Server ein.
4. Geben Sie im Feld **Hostname oder URL** die UEM-Server-URL mit dem Format `<http or https>://<servername>:<port>` ein, wobei die Standardportnummer 8885 lautet.
5. Klicken Sie auf **Weiter**.
6. Schließen Sie das **Server**-Fenster.

**Wenn Sie fertig sind:** [Vorbereiten von iOS-Geräten mit Apple Configurator 2](#).

## Vorbereiten von iOS-Geräten mit Apple Configurator 2

Wenn Sie ein Gerät vorbereiten, bereinigt Apple Configurator 2 das Gerät und aktualisiert das Betriebssystem auf die neueste Version.

**Bevor Sie beginnen:** [Hinzufügen von BlackBerry UEM-Serverinformationen zu Apple Configurator 2.](#)

1. Öffnen Sie Apple Configurator 2.
2. Verbinden Sie ein oder mehrere iOS-Geräte mit Ihrem Computer.
3. Klicken Sie auf **Vorbereiten**.
4. Wählen Sie in der Dropdown-Liste **Konfiguration** die Option **Manuell** aus. Klicken Sie auf **Weiter**.
5. Wählen Sie in der Dropdown-Liste **Server** den BlackBerry UEM-Server aus. Klicken Sie auf **Weiter**.
6. Aktivieren Sie ggf. das Kontrollkästchen **Unter Aufsicht stellen**. Klicken Sie auf **Weiter**.
7. Wenn Sie **Unter Aufsicht stellen** ausgewählt haben, vervollständigen Sie die Unternehmensinformationen.
8. Klicken Sie auf **Vorbereiten**, und warten Sie, während das Gerät vorbereitet wird. Dieser Prozess dauert bis zu 15 Minuten.

**Wenn Sie fertig sind:** Verteilen Sie die Geräte an die Benutzer zur Aktivierung.

# Importieren oder exportieren einer Liste genehmigter Geräte-IDs

Sie können eine Liste eindeutiger Gerätekennungen importieren und exportieren, um zu beschränken, welche Geräte bei BlackBerry UEM registriert werden können. Derzeit ist die einzige eindeutige Kennung, die UEM unterstützt, die Seriennummer des Geräts.

**Bevor Sie beginnen:** Stellen Sie beim Import einer Liste sicher, dass Sie über eine CSV-Datei verfügen, die eine Liste der eindeutigen Gerätekennungen enthält.

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Einstellungen > Allgemeine Einstellungen > Aktivierungsstandards**.
2. Klicken Sie im Abschnitt **Geräte-IDs importieren oder exportieren** neben dem Feld **Bestätigte Geräte-IDs hochladen (.csv)** auf **Durchsuchen**.
3. Navigieren Sie zur .csv-Datei.
4. Klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Speichern**.

**Wenn Sie fertig sind:** Um die Liste zu exportieren, klicken Sie auf **Genehmigte Geräte-IDs exportieren (.csv)**.

# Deaktivieren von Geräten

Wenn ein Gerät deaktiviert wird, 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.

Ein Gerät kann mit einer der folgenden Methoden deaktiviert werden:

- Administratoren können ein Gerät von der UEM-Verwaltungskonsole aus mit dem Befehl „Nur geschäftliche Daten löschen“ oder „Alle Gerätedaten löschen“ deaktivieren.
- UEM kann ein Gerät deaktivieren, wenn es gegen die Regeln des zugewiesenen Konformitätsprofils verstößt und die konfigurierte Erzwingungsaktion darin besteht, das Gerät zu deaktivieren.
- Benutzer können ein Gerät von UEM Self-Service mit dem Befehl „Nur geschäftliche Daten löschen“ oder „Alle Gerätedaten löschen“ deaktivieren.
- Benutzer können die UEM Client verwenden, um iOS- und Android-Geräte zu deaktivieren.
- Benutzer können Windows 10-Geräte unter „Einstellungen > Konten > Geschäftlicher Zugriff > Löschen“ deaktivieren.

Beachten Sie folgende Hinweise, wenn Sie Geräte mit den angegebenen Aktivierungsarten deaktivieren:

Aktivierungsart	Überlegungen
Android Enterprise-Geräte mit nur einem Arbeitsprofil	Sie haben die Möglichkeit, alle Daten von der SD-Karte zu löschen und den werkseitigen Rücksetzschutz aufzuheben.
Android Enterprise-Geräte mit Geschäftlich und persönlich – vollständige Kontrolle-Aktivierungen	<ul style="list-style-type: none"> <li>• Der Befehl „Alle Gerätedaten löschen“ wird nur für Android 10 unterstützt. UEM unterstützt Android 10 ab Januar 2024 nicht mehr.</li> <li>• Der Befehl „Nur geschäftliche Daten löschen“ wird für Android 11 und höher unterstützt. Dieser Befehl entfernt alle geschäftlichen Daten und Apps. Der Benutzer kann jedoch persönliche Daten und Apps behalten und das nicht verwaltete Gerät weiterhin verwenden.</li> </ul>
Android Enterprise-Geräte mit Geschäftlich und persönlich – Benutzer-Datenschutz- und Geschäftlich und persönlich – vollständige Kontrolle-Aktivierungen	Wenn Sie den Befehl „Nur geschäftliche Daten löschen“ verwenden, können Sie einen Grund angeben, der in der Benachrichtigung auf dem Gerät des Benutzers angezeigt wird. Wenn das Gerät aufgrund eines Verstoßes gegen die Konformitätsregeln deaktiviert wird, gibt die Benachrichtigung den Grund an, warum das Gerät nicht richtlinienkonform war.
Knox MDM	<ul style="list-style-type: none"> <li>• Interne Apps werden deinstalliert.</li> <li>• Die Option „Deinstallieren“ wird für beliebige öffentliche Apps, die von der App-Liste aus installiert wurden, nach Bedarf verfügbar.</li> </ul>
Samsung Knox Workspace-Geräte mit Geschäftlich und persönlich – vollständige Kontrolle	Bei Deaktivierung des Geräts werden alle Daten vom Gerät gelöscht. Sie können mit der IT-Richtlinienregel „Löschen von Daten bei Deaktivierung“ angeben, welche Daten gelöscht werden.

# Fehlerbehebung der Geräteaktivierung

Zur Fehlersuche bei der Aktivierung für Geräte jeden Typs überprüfen Sie stets Folgendes:

- Stellen Sie sicher, dass Lizenzen für den Gerätetypen und den Aktivierungsarten verfügbar sind.
- Stellen Sie sicher, dass das dem Gerät zugewiesene Aktivierungsprofil den Gerätetypen unterstützt.
- Überprüfen Sie die Netzwerkverbindung auf dem Gerät.
  - Stellen Sie sicher, dass das Mobilfunknetz bzw. das Wi-Fi-Netzwerk aktiv ist und ausreichender Empfang gegeben ist.
  - Wird das geschäftliche Wi-Fi verwendet, vergewissern Sie sich, dass der Gerätenetzwerkpfad verfügbar ist.
  - Wenn ein Benutzer ein VPN-Profil oder ein geschäftliches Wi-Fi-Profil manuell konfigurieren muss, um auf Inhalte hinter der Firewall Ihres Unternehmens zugreifen zu können, vergewissern Sie sich, dass die Profile auf dem Gerät richtig konfiguriert sind.
- Wenn Sie Konformitätsregeln für Geräte mit gerootetem Betriebssystem, unzulässige Betriebssystemversionen oder unzulässige Gerätemodelle konfiguriert haben, stellen Sie sicher, dass das Gerät regelkonform ist.
- Wenn UEM lokal installiert ist und das Gerät versucht, eine Verbindung mit UEM oder der BlackBerry Infrastructure über die Firewall des Unternehmens herzustellen, vergewissern Sie sich, dass die richtigen Firewall-Ports geöffnet sind.
- Sammeln Sie Geräteprotokolle. Weitere Informationen zum Abrufen von Geräteprotokollen finden Sie unter [KB 36986](#) für iOS und [KB 32516](#) für Android.

## Android Management-Geräte

- Sie müssen separate Aktivierungsprofile für Android Enterprise und Android Management erstellen. Wenn die Aktivierungsarten Android Enterprise und Android Management im selben Profil angegeben sind, hat die Art Android Management Vorrang, selbst wenn er niedriger als Android Enterprise eingestuft ist. Nur das Kennwort und die Aktivierungsinformationen für die Aktivierungsart Android Management werden in den QR-Code eingebettet.
- Bei einigen Geräten wird möglicherweise ein unnötiger Bildschirm „Einrichtung und Wiederherstellung“ angezeigt, nachdem das Gerät den Aktivierungsvorgang erfolgreich abgeschlossen hat.

## Knox Workspace- und Android Enterprise-Geräte

Wenn Sie Fehler bei der Aktivierung von Samsung-Geräten beheben, die Samsung Knox Workspace verwenden, stellen Sie sicher, dass die Containerversion von Knox unterstützt wird. Knox Workspace Erfordert Knox Container 2.0 oder höher.

Wenn Sie Fehler bei der Aktivierung von Android Enterprise-Geräten beheben, stellen Sie sicher, dass das UEM-Benutzerkonto dieselbe E-Mail-Adresse wie in der Google-Domäne hat. Wenn die E-Mail-Adressen nicht übereinstimmen, wird auf dem Gerät dieser Fehler angezeigt: „Gerät kann nicht aktiviert werden – Nicht unterstützte Aktivierungsart.“

# Fehlerbehebung: Aktivierungsfehler und -probleme

## Aktivierungsfehler

Fehler	Mögliche Lösung
Die Geräteaktivierung kann nicht abgeschlossen werden, da der Server keine Lizenzen hat. Wenden Sie sich bitte an Ihren Administrator.	Stellen Sie in der UEM-Verwaltungskonsole sicher, dass Lizenzen verfügbar sind. Aktivieren Sie ggf. Lizenzen oder kaufen Sie zusätzliche Lizenzen.
Das Profil konnte nicht installiert werden. Das Zertifikat „AutoMDMCert.pfx“ konnte nicht importiert werden.	Dieser Fehler wird auf einem iOS-Gerät angezeigt, wenn bereits ein Profil auf dem Gerät vorhanden ist.  Wechseln Sie auf dem Gerät zu <b>Einstellungen &gt; Allgemeine Einstellungen &gt; Profil</b> , und überprüfen Sie, ob bereits ein Profil vorhanden ist. Entfernen Sie das Profil, und versuchen Sie erneut zu aktivieren. Wenn der Fehler weiterhin besteht, müssen Sie das Gerät möglicherweise zurücksetzen, da eventuell Daten zwischengespeichert wurden.
Profilinstallation nicht erfolgreich: Die neue MDM-Nutzlast stimmt nicht mit der alten Nutzlast überein.	Dieser Fehler wird auf einem iOS-Gerät angezeigt, wenn bereits ein Profil auf dem Gerät vorhanden ist.  Wechseln Sie auf dem Gerät zu <b>Einstellungen &gt; Allgemeine Einstellungen &gt; Profil</b> , und überprüfen Sie, ob bereits ein Profil vorhanden ist. Entfernen Sie das Profil, und versuchen Sie erneut zu aktivieren. Wenn der Fehler weiterhin besteht, müssen Sie das Gerät möglicherweise zurücksetzen, da eventuell Daten zwischengespeichert wurden.
Fehler 3007: Server nicht verfügbar.	Dieser Fehler kann auftreten, wenn das Zertifikat, das UEM zum Signieren des MDM-Profiles verwendet, das es an ein iOS-Gerät sendet, von diesem Gerät nicht als vertrauenswürdig eingestuft wird (der Benutzer wird aufgefordert, diesem Zertifikat zu vertrauen, wenn er das Gerät aktiviert). Installieren Sie in einer lokalen Umgebung das Stammzertifikat für die Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Weitere Informationen finden Sie unter <a href="#">Ändern der Zertifikate, die BlackBerry UEM für die Authentifizierung verwendet</a> , in der Dokumentation zur Konfiguration.  Dieser Fehler kann auch auftreten, wenn Sie einen transparenten Proxy wie Blue Coat verwenden, der Port 443 für nichtstandardmäßigen Datenverkehr überwacht, und der UEM Client die erforderlichen HTTP CONNECT- und HTTP OPTIONS-Anrufe an UEM nicht tätigen kann. Stellen Sie sicher, dass Ihre Proxykonfiguration den UEM Client nicht daran hindert, diese Aufrufe zu tätigen.

Fehler	Mögliche Lösung
<p>Serververbindung konnte nicht hergestellt werden, bitte überprüfen Sie die Konnektivität und die Serveradresse.</p>	<p>Dieser Fehler kann auftreten, wenn der Benutzername (oder die Kundenadresse, wenn die Registrierung mit BlackBerry Infrastructure deaktiviert wurde) nicht korrekt eingegeben wurde oder wenn das Aktivierungskennwort nicht festgelegt wurde oder abgelaufen ist.</p> <p>Überprüfen Sie, ob Benutzername, Kennwort und Kundenadresse (falls zutreffend) korrekt sind, oder legen Sie ein neues Aktivierungskennwort mit UEM Self-Service fest, und versuchen Sie es erneut.</p>

## Aktivierungsprobleme

Problem	Mögliche Lösung
<p>iOS- oder macOS-Geräteaktivierungen schlagen bei ungültigen APNs-Zertifikaten fehl.</p>	<p>Das APNs-Zertifikat ist möglicherweise nicht richtig registriert. Führen Sie eine oder mehrere der folgenden Aktionen aus:</p> <ul style="list-style-type: none"> <li>• Klicken Sie in der Menüleiste der Verwaltungskonsole auf <b>Einstellungen &gt; Externe Integration &gt; Apple Push Notification</b>. Vergewissern Sie sich, dass das APNs-Zertifikat den Status „Installiert“ aufweist. Wenn der Status nicht korrekt ist, versuchen Sie, das APNs-Zertifikat erneut zu registrieren.</li> <li>• Zum Testen der Verbindung zwischen UEM und dem APNs-Server klicken Sie auf <b>APNs-Zertifikat testen</b>.</li> <li>• Rufen Sie ggf. eine neue signierte CSR von BlackBerry ab, fordern Sie ein neues APNs-Zertifikat an, und registrieren Sie es. Weitere Informationen finden Sie unter <a href="#">Abrufen eines APNs-Zertifikats für die Verwaltung von iOS- und macOS-Geräten</a> in der Dokumentation zur Konfiguration.</li> </ul>
<p>Die Benutzer erhalten keine Aktivierungs-E-Mail.</p>	<p>Wenn Sie den Mailserver eines Drittanbieters nutzen, werden E-Mail-Nachrichten von UEM eventuell als Spam markiert und in den Spam-E-Mail-Ordner oder den Junk-E-Mail-Ordner verschoben.</p>
<p>Der Bildschirm mit den Benutzerdetails in UEM zeigt mehr aktivierte Windows-Geräte als erwartet an.</p>	<p>Wenn ein Benutzer BlackBerry Access und BlackBerry Work für Windows auf einem Computer installiert, werden diese Apps auf dem Bildschirm mit den Benutzerdetails als Windows-Gerät angezeigt. Dies ist das erwartete Verhalten.</p>

# Rechtliche Hinweise

©2024 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

Patente, sofern zutreffend, zu finden unter: [www.blackberry.com/patents](http://www.blackberry.com/patents).

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.

SO FERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIE, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIE, 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, SO FERN SIE NICHT WIE OBEN DARGELEGT AUSGESCHLOSSEN WERDEN KÖNNEN, HIERMIT AUF 90 TAGE AB DATUM DES ERWERBS DER DOKUMENTATION ODER DES ARTIKELS, AUF DEN SICH DIE FORDERUNG BEZIEHT, BESCHRÄNKT.

IN DEM DURCH DAS IN IHREM RECHTSGEBIET ANWENDBARE GESETZ MAXIMAL ZULÄSSIGEN AUSMASS HAFTET BLACKBERRY UNTER KEINEN UMSTÄNDEN FÜR SCHÄDEN JEDLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEDLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTE UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE,

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 ANGEHÖRENDE UNTERNEHMEN IN KEINER WEISE IM ZUSAMMENHANG MIT DER DOKUMENTATION.

Bevor Sie Drittprodukte bzw. -dienste abonnieren, installieren oder verwenden, müssen Sie sicherstellen, dass Ihr Mobilfunkanbieter sich mit der Unterstützung aller zugehörigen Funktionen einverstanden erklärt hat. Einige Mobilfunkanbieter bieten möglicherweise keine Internet-Browsing-Funktion in Zusammenhang mit einem Abonnement für den BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem 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 GARANTIEEN, 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