# BlackBerry UEM

## Übersicht und neue Funktionen

12.12

# Inhalt

# Neuerungen in BlackBerry UEM 12.12

### iOS

- **Fehlermeldung zur Aktualisierung von Apple DEP**: Wenn Sie die aktualisierten Geschäftsbedingungen für Apple Business Manager noch nicht akzeptiert haben, erhalten Sie eine Fehlermeldung per E-Mail.
- **Manuelle Synchronisierung der Apple DEP-Konten mit Apple Business Manager**: Sie können Apple DEP-Konten in BlackBerry UEM manuell synchronisieren, um die Gerätekonnektivität zu gewährleisten.
- **Aktualisierung der Ereignisbenachrichtigung**: Die Ereignisbenachrichtigung über den Zustand der Apple DEP-Verbindung enthält jetzt Details für den Kommunikationsstatus, den Betriebsmodus und die Uhrzeit der letzten Synchronisierung.
- **Aktualisieren von iOS auf eine bestimmte Versionsnummer**: Auf der Registerkarte „Gerät" können Sie die Softwareversion auf einem überwachten iOS-Gerät auf eine bestimmte Versionsnummer aktualisieren. Sie können diese Funktion verwenden, um das Gerätebetriebssystem auf eine Version zu aktualisieren, die von der IT-Abteilung Ihres Unternehmens zertifiziert wurde.
- **Unterstützung für SSO-Erweiterung unter iOS 13**: Die SSO-Erweiterung für iOS 13 und iPadOS 13 ermöglicht es Benutzern, sich einmal zu authentifizieren und sich dann automatisch bei Domänen und Webservices innerhalb des Unternehmensnetzwerks anzumelden. Sie können ein SSO-Erweiterungsprofil in BlackBerry UEM für Geräte mit iOS (oder iPadOS) 13 konfigurieren.
- **Verbesserter Aktivierungsprozess**: Der BlackBerry UEM Client für iOS wurde mit Sicherheitsmerkmalen aktualisiert, um die Fälle zu minimieren, in denen ein Benutzer den Aktivierungsprozess von Anfang an aufgrund einer Unterbrechung während der Geräteaktivierung neu starten muss (z. B. wenn der Benutzer während der Aktivierung einen Anruf erhält). Wenn der Benutzer zu UEM Client zurückkehrt, kann er nun die Aktivierung vom letzten Schritt an fortsetzen.
- **Neue Aktivierungsart für iOS- und iPadOS 13.1-Geräte**: Eine neue Aktivierungsart „Benutzerdatenschutz - Benutzerregistrierung" ist nun für nicht überwachte iOS-Geräte mit iOS oder iPadOS 13.1 und höher verfügbar. Die Aktivierungsart trägt dazu bei, die Privatsphäre des Benutzers zu wahren, während die geschäftlichen Daten getrennt und geschützt bleiben. Administratoren können geschäftliche Daten verwalten (z. B. geschäftliche Daten löschen), ohne dass Auswirkungen auf persönliche Daten erfolgen. Um ein Gerät mit dieser Aktivierungsart zu aktivieren, können Benutzer einfach den in der Aktivierungs-E-Mail erhaltenen QR Code mit der nativen Kamera-App scannen und das MDM-Profil manuell auf das Gerät herunterladen und installieren. Um das Gerät zu aktivieren, meldet sich der Benutzer bei seinem verwalteten Apple ID-Konto an. Administratoren können zudem den BlackBerry UEM Client zuweisen, um Benutzern die einfache Aktivierung anderer BlackBerry Dynamics-Apps, das Importieren von Zertifikaten, die Verwendung von 2FA-Funktionen und die Verwendung von CylancePROTECT Mobile for BlackBerry UEM zu ermöglichen und deren Konformitätsstatus zu prüfen.
- **Unterstützung für iOS 13-Funktionen**: BlackBerry UEM unterstützt die neuen Funktionen in iOS 13. Die Unterstützung umfasst drei neue IT-Richtlinienregeln, Unterstützung für WPA-3 Personal- und WPA-3 Enterprise Wi-Fi-Sicherheit sowie neue Profileinstellungen für E-Mail, VPN-Profil und App-Sperrmodus.

### Android

- **Profil für den werkseitigen Rücksetzschutz**: Sie können für mehrere Google-Konten ein Profil für den werkseitigen Rücksetzschutz festlegen.
- **Verbesserte Benutzererfahrung bei der Android Enterprise-Geräteaktivierung**: Die Anzahl der erforderlichen Schritte zur Aktivierung von Android Enterprise-Geräten wurde reduziert. Benutzer können jetzt auf ein Kontrollkästchen tippen, wenn sie ihren Benutzernamen eingeben, um die Lizenzvereinbarung zu akzeptieren. Zusätzliche Benachrichtigungen wurden hinzugefügt, um den Fortschritt der App-Installation anzuzeigen. Es wurden zusätzliche Meldungen hinzugefügt, die die für UEM Client erforderlichen Berechtigungen beschreiben.
- **Aktualisierte Aktivierungsfehlermeldungen**: Wenn die Aktivierung auf einem Android-Gerät nicht erfolgreich war, wird eine neue oder aktualisierte Fehlermeldung angezeigt, die erklärt, warum das Gerät nicht

ordnungsgemäß aktiviert wurde. Dadurch können Benutzer und IT-Mitarbeiter das Problem diagnostizieren und beheben.

- **Verwenden von OEMConfig-Apps von Android-Geräteherstellern zum Verwalten von Gerätefunktionen**: BlackBerry UEM unterstützt die Verwendung von OEMConfig-Apps von Geräteherstellern (z. B. Samsung Knox Service Plugin) zur Verwaltung von herstellerspezifischen APIs auf Geräten. Mit dem Samsung Knox Service-Plug-in können Sie neue Samsung-Gerätefunktionen verwalten, sobald Samsung Geräte oder Apps aktualisiert, anstatt bis zur nächsten UEM-Aktualisierung auf neue Profileinstellungen und IT-Richtlinienregeln zu warten.
- **Feedback von Android-Apps mit App-Konfigurationen anzeigen**: BlackBerry UEM empfängt und zeigt Fehler- und Informationsfeedback von Android-Apps an, die über eine App-Konfiguration verfügen und für Feedback entwickelt wurden.
- **Einfaches Hinzufügen geschäftlicher Apps für Android Enterprise-Geräte zu Google Play**: Zugriff auf die aktualisierte Google Play-Benutzeroberfläche von BlackBerry UEM aus, um private Apps und Web-Apps (Verknüpfungen zu Webseiten) zu Google Play im geschäftlichen Profil auf Android Enterprise-Geräten hinzuzufügen.
- **Unterstützung für COSU-Geräte (unternehmenseigene Einzweckgeräte) für Android Enterprise**: BlackBerry UEM unterstützt nun unternehmenseigene Einzweckgeräte für Android Enterprise ab Version 7.0. Ein Gerät mit COSU-Konfiguration ist für eine bestimmte Reihe von Anwendungen gesperrt bzw. auf eine bestimmte Funktion beschränkt.
- **Fehlerbericht anfordern**: Sie können jetzt einen Befehl von BlackBerry UEM an ein Android Enterprise-Gerät senden, um die Client-Protokolle anzufordern. Für die folgenden Aktivierungsarten kann ein Fehlerbericht angefordert werden:
  - Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)
  - Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil)
- **Steuern von Laufzeitberechtigungen für Android-Apps**: Wenn Sie eine Android-App in BlackBerry UEM hinzufügen, können Sie Laufzeitberechtigungen für die App festlegen. Sie können für die jeweilige für die App aufgeführte Berechtigung Berechtigungen erteilen, Berechtigungen verweigern oder eine App-Berechtigungsrichtlinie verwenden.
- **Client-Downloadverzeichnis mit QR Code** senden: Sie können den Speicherort zum Herunterladen des UEM Client für Aktivierungsarten nur für den geschäftlichen Bereich definieren (vollständig verwaltetes Android Enterprise-Gerät). Das Verzeichnis wird im QR Code gesendet.

#### Samsung Knox

- **Unterstützung für Samsung Knox DualDAR**: Geräte, die Samsung Knox DualDAR-Verschlüsselung unterstützen, können Knox Workspace-Daten nun mit zwei Verschlüsselungsschichten sichern. Wenn der Benutzer das Gerät nicht verwendet, sind alle Daten in Knox Workspace gesperrt und können nicht von im Hintergrund ausgeführten Apps aufgerufen werden. Im Aktivierungsprofil können Sie angeben, ob Sie die standardmäßige DualDAR-App oder eine interne App zum Verschlüsseln des Arbeitsbereichs verwenden möchten. Im Geräteprofil können Sie das Zeitlimit für die Datensperre festlegen, nach dem der Benutzer sich sowohl bei dem Gerät als auch beim Arbeitsbereich authentifizieren muss, um wieder auf geschäftliche Daten zuzugreifen. Außerdem können Sie Apps festlegen, die auf geschäftliche Daten zugreifen dürfen, selbst wenn geschäftliche Daten gesperrt sind.

  Die Samsung Knox DualDAR-Verschlüsselung wird auf Geräten mit Samsung Knox ab Version 3.3 für neue Aktivierungen mit der Premium-Aktivierungsart „Geschäftlich und persönlich - vollständige Kontrolle“ (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil) unterstützt.
- **Verbesserte Unterstützung für Knox Platform for Enterprise-Geräte**: Samsung Knox-IT-Richtlinien wurden für Geräte hinzugefügt, die Knox Platform for Enterprise unterstützen. Diese Richtlinien werden je nach ausgewählter Android Enterprise-Aktivierungsart auf das Gerät, den persönlichen Bereich oder den geschäftlichen Bereich auf dem Gerät angewendet. Außerdem wurde Unterstützung für natives Samsung-VPN

und E-Mail hinzugefügt, die Möglichkeit, Apps im persönlichen Bereich einzuschränken und den geschäftlichen Bereich per Fernzugriff zu sperren. Um Knox Platform for Enterprise-Funktionen verwenden zu können, ist auf dem Knox-Gerät Android 8 oder höher sowie eine der Android Enterprise-Aktivierungsarten mit Premium-Option erforderlich.

#### Software-Unterstützung

Ab Version 12.12 wird die folgende Software von BlackBerry UEM nicht mehr unterstützt:

- iOS Version 11: (weitere Informationen finden Sie unter support.blackberry.com im Artikel KB57538)
- Android OS Version 6 (weitere Informationen finden Sie unter support.blackberry.com im Artikel KB57539)
- BlackBerry 10 OS (weitere Informationen finden Sie unter Übersicht zum Lebenszyklus der BlackBerry-Software)
- Windows Server 2008

#### Verwaltungskonsole

- **Konformitätsprofilaktualisierungen**: In einem Konformitätsprofil können Sie jetzt die Erzwingungsaktion für BlackBerry Dynamics-Apps auf Überwachen und Protokollieren setzen. „Überwachen und Protokollieren“ ist jetzt die Standardeinstellung für Konformitätsprofile. Die Standardoption für die Aktion „Aktion bei Ablauf des Aufforderungsintervalls“ ist ebenfalls „Überwachen und Protokollieren“.
- **Verbesserungen bei der Gerätefilterung**: Sie können Geräte jetzt nach Modellnummer filtern. Sie können jetzt beispielsweise nach unterschiedlichen Samsung Galaxy-Gerätemodellen wie Samsung A5 SM-A520F und Samsung A5 SM-A510F filtern. Auf diese Weise können Administratoren Richtlinien, Profile und Gruppenstatus auf mehrere Geräte eines bestimmten Modells anwenden.
- **App-Konfiguration**: Wenn Sie eine neue Version einer internen App zu BlackBerry UEM hinzufügen, wird die App-Konfiguration automatisch von der älteren Version der internen App in die neue Version kopiert.
- **Aktualisierung der Ereignisbenachrichtigung**: Die Ereignisbenachrichtigung „Aktualisierung von Metadaten“ wurde verbessert und zeigt nun den vollständigen Namen des Gerätehardwareanbieters an.
- **Überschreiben von BlackBerry Dynamics-Konnektivitätsprofilen auf App-Basis**: Sie können jetzt ein BlackBerry Dynamics-Konnektivitätsprofil angeben, das mit der jeweiligen BlackBerry Dynamics-App in BlackBerry UEM verknüpft werden soll. Wenn ein Profil einer App zugewiesen wird, hat dieses Profil Vorrang vor dem Profil, das dem Benutzer dieser App zugewiesen wurde.
- **App-Verknüpfungsfilter**: Mit einem neuen Filter auf der App-Seite der UEM-Verwaltungskonsole können Sie nach App-Verknüpfungen suchen.
- **Dedizierte Gerätegruppen**: BlackBerry UEM enthält eine neue Menüoption „Dedizierte Geräte“. Sie können freigegebene Gerätegruppen und öffentliche Gerätegruppen im Menü „Dedizierte Geräte“ anzeigen, hinzufügen, bearbeiten und löschen. Öffentliche Gerätegruppen werden zur Verwaltung von zweckbestimmten Geräten verwendet, die nicht bestimmten Benutzern zugewiesen sind. Freigegebene Gerätegruppen werden zur Verwaltung von Geräten verwendet, die von mehreren Benutzern ausgecheckt werden können. Zuvor waren freigegebene Gerätegruppen unter dem Menüpunkt „Benutzer“ zu finden.

#### BlackBerry Dynamics

- **BlackBerry Dynamics-Proxy-Einstellungen mit PAC-Datei konfigurieren**: Sie können jetzt eine PAC-Datei verwenden, um HTTP-Proxy-Einstellungen für Verbindungen des App-Datenverkehrs zu BlackBerry Dynamics NOC konfigurieren. PAC-Dateien werden nur für Apps unterstützt, die BlackBerry Dynamics SDK ab Version 7.0 verwenden.

**Neue IT-Richtlinienregeln**

| Gerätetyp | Gruppe | Name | Beschreibung | Aktivierungsarten | Standardwert |
|---|---|---|---|---|---|
| iOS | Apps | Verwendung von USB durch Dateien-App zulassen (nur unter Aufsicht) | Legen Sie fest, ob die Dateien-App über eine USB-Verbindung auf Dateien zugreifen kann. | MDM-Steuerelemente | Ausgewählt |
| iOS | Apps | Verbindung zu Netzlaufwerken über Dateien-App zulassen (nur unter Aufsicht) | Legen Sie fest, ob die Dateien-App auf Dateien zugreifen kann, die auf einem Netzlaufwerk gespeichert sind. | MDM-Steuerelemente | Ausgewählt |
| iOS | Gerätefunktionalität | Aktivierung von Wi-Fi erzwingen (nur unter Aufsicht) | Legen Sie fest, ob Wi-Fi auf dem Gerät immer aktiviert ist. Wenn diese Regel ausgewählt ist, können Benutzer Wi-Fi nicht über die Geräteeinstellungen oder das Control Center ausschalten, und Wi-Fi wird im Flugmodus nicht deaktiviert. | MDM-Steuerelemente | Nicht ausgewählt |
| iOS | Apps | Verbindung zu Netzlaufwerken über Dateien-App zulassen (nur unter Aufsicht) | Legen Sie fest, ob die Dateien-App auf Dateien zugreifen kann, die auf einem Netzlaufwerk gespeichert sind. | MDM-Steuerelemente | Ausgewählt |
| iOS | Gerätefunktionalität | Aktivierung von Wi-Fi erzwingen | Legen Sie fest, ob Wi-Fi auf dem Gerät | MDM-Steuerelemente | Nicht ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | (nur unter Aufsicht) | immer aktiviert ist. Wenn diese Regel ausgewählt ist, können Benutzer Wi-Fi nicht über die Geräteeinstellungen oder das Control Center ausschalten, und Wi-Fi wird im Flugmodus nicht deaktiviert. | | |
| Android | Global (nur Samsung Knox-Geräte) - Apps | Ausgehende SMS zulassen | Legen Sie fest, ob ein Gerät SMS-Nachrichten senden kann. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Apps | Eingehende SMS zulassen | Legen Sie fest, ob ein Gerät SMS-Nachrichten empfangen kann. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Interne Speicherverschlüsselung erforderlich | Legen Sie fest, ob der Benutzer dazu aufgefordert wird, den Gerätespeicher und die interne SD-Karte des Geräts zu verschlüsseln. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | USB-Fehlerbehebung aktivieren | Legen Sie fest, ob die Fehlerbehebung über eine USB-Verbindung verfügbar ist. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| Android | Global (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Benutzern die Änderung des Pseudostandorts gestatten | Legen Sie fest, ob ein Benutzer die Angabe eines falschen GPS-Standorts auf dem Gerät aktivieren oder deaktivieren kann. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Kennwort | Maximale Länge einer Zahlenfolge | Legen Sie die maximale Länge der Zahlenfolge fest, die im Gerätekennwort zulässig ist. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | |
| Android | Global (nur Samsung Knox-Geräte) - Kennwort | Mindestanzahl geänderter Zeichen für neue Gerätekennwörter | Legen Sie die Mindestanzahl geänderter Zeichen fest, die ein neues Kennwort im Vergleich zu einem vorherigen Kennwort enthalten muss. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | |
| Android | Global (nur Samsung Knox-Geräte) - Kennwort | Sichtbarkeit des Gerätekennworts zulassen | Legen Sie fest, ob das Gerätekennwort bei der Eingabe sichtbar sein soll. | Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Kennwort | Sperrbildschirmmeldung anfordern | Legen Sie fest, ob eine Meldung angezeigt werden soll, wenn das Gerät gesperrt wird. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer eine Meldung für den | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | Sperrbildschirm auswählen. | | |
| Android | Global (nur Samsung Knox-Geräte) - Kennwort | Sperrbildschirmmeldung | Legen Sie den Text fest, der auf dem Bildschirm beim Sperren des Geräts angezeigt werden soll. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | |
| Android | Global (nur Samsung Knox-Geräte) - Kennwort | Maximallänge für Zeichenfolge | Legen Sie die maximale Länge der Zeichenfolge fest, die im Gerätekennwort zulässig ist. Gilt nur, wenn die Qualität des Gerätekennworts alphabetisch, alphanumerisch oder komplex ist. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | |
| Android | Global (nur Samsung Knox-Geräte) - Apps | Telefon zulassen | Legen Sie fest, ob ein Benutzer das Telefon verwenden kann.<br>Wenn diese Regel nicht ausgewählt ist, kann der Benutzer mit dem Gerät nur Notrufe tätigen. Alle anderen Anrufe werden gesperrt. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Datums- und Uhrzeitänderungen zulassen | Legen Sie fest, ob Benutzer die Einstellung für Datum und Uhrzeit auf einem Gerät ändern können. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Automatische Zeitsynchronisierung erzwingen | Legen Sie fest, ob das Gerät mithilfe von NITZ das Datum und die Uhrzeit automatisch abrufen kann. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer auswählen, ob das Gerät Datum und Uhrzeit automatisch synchronisiert. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Natives Samsung VPN zulassen | Legen Sie fest, ob ein Benutzer die systemeigene VPN-Funktionalität nutzen kann. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer keine VPN-Sitzung öffnen oder auf die VPN-Einstellungen in der App „Einstellungen“ zugreifen. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | WAP-Push beim Roaming zulassen | Legen Sie fest, ob ein Gerät beim Roaming WAP-Push-Nachrichten empfangen kann. Wenn diese Regel nicht ausgewählt ist, kann das Gerät beim Roaming keine MMS- | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | Nachrichten empfangen. Der Benutzer kann diese Einstellung nicht auf dem Gerät ändern. Diese Regel gilt nur, wenn das Gerät sich im Roaming-Modus befindet. | | |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Automatische Synchronisierung beim Roaming zulassen | Legen Sie fest, ob das Gerät während des Roamings automatisch Daten synchronisieren kann. Wenn diese Regel nicht ausgewählt ist, kann ein Gerät im Roaming-Modus Daten nur synchronisieren, wenn der Benutzer auf ein Konto zugreift. Der Benutzer kann diese Einstellung nicht auf dem Gerät ändern. Diese Einstellung gilt nur, wenn sich das Gerät im Roaming-Modus befindet. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Anrufe beim Roaming zulassen | Legen Sie fest, ob ein Gerät beim Roaming Sprachanrufe tätigen oder | Nur geschäftlicher Bereich, Geschäftlich und persönlich – | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | empfangen kann. | vollständige Kontrolle | |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | SD-Karte zulassen | Legen Sie fest, ob ein Gerät auf eine SD-Karte zugreifen kann. Wenn diese Regel nicht ausgewählt ist, wird der Lese- und Schreibzugriff auf die SD-Karte gesperrt. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Daten im Mobilfunknetz zulassen | Legen Sie fest, ob ein Gerät eine Mobilfunknetzverbindung verwenden kann. Wenn diese Regel nicht ausgewählt ist, kann das Gerät die SIM-Datenverbindung nicht verwenden. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Hinzufügen neuer Wi-Fi-Netzwerke durch Benutzer zulassen | Legen Sie fest, ob Benutzer dem Gerät neue Wi-Fi-Profile hinzufügen können. Wenn diese Regel nicht ausgewählt ist, können Benutzer nur die von Ihnen konfigurierten geschäftlichen Wi-Fi-Profile verwenden. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Android zulassen Beam | Legen Sie fest, ob Benutzer Android Beam oder S Beam verwenden | Nur geschäftlicher Bereich, Geschäftlich und | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | können, um Kontaktinformationen, Web-Lesezeichen und andere Daten an Geräte in der Nähe zu senden. | persönlich – vollständige Kontrolle | |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | Media Transfer Protocol (MTP) zulassen | Legen Sie fest, ob ein Gerät MTP verwenden kann. Da Android die USB-Dateiübertragung nur über MTP unterstützt, können Sie mit dieser Regel alle Arten der Dateiübertragung über USB blockieren. Picture Transfer Protocol (PTP) ist eine Untergruppe von MTP und ist von dieser Regel ebenfalls betroffen. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Global (nur Samsung Knox-Geräte) - Gerätefunktionalität | USB-Hostspeicher zulassen | Legen Sie fest, ob ein Gerät USB-Hostspeicher mittels USB OTG verwenden kann. Ist diese Regel ausgewählt, kann ein Benutzer USB-Sticks (tragbare USB-Speicher), externe Festplatten oder SD Card Reader | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | anschließen, die auf dem Gerät als Speicherlaufwerk genutzt werden können. Ist diese Regel nicht ausgewählt, kann der Benutzer keine externen Speichergeräte installieren. | | |
| Android | Persönliches Profil (nur Samsung Knox-Geräte) - Gerätefunktionalität | Audioaufnahme zulassen | Legen Sie fest, ob mit einem Gerät Audioaufnahmen gemacht werden können. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer dennoch Anrufe tätigen und Audio-Streaming mit dem Gerätemikrofon nutzen. Die Regel gilt für Telefonanrufe, Spracherkennung und VoIP. Videoaufnahmen sind weiterhin zulässig, solange kein Audioaufnahmeversuch erfolgt. | Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Persönliches Profil (nur Samsung Knox-Geräte) - Gerätefunktionalität | Videoaufnahme zulassen | Legen Sie fest, ob mit einem Gerät Videoaufnahmen gemacht werden können. Wenn diese Regel nicht ausgewählt ist, | Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | ist die Kamera dennoch verfügbar, und der Benutzer kann fotografieren und Video-Streaming nutzen. Wenn diese Regel nicht ausgewählt ist, werden alle laufenden Videoaufnahmen unterbrochen. | | |
| Android | Persönliches Profil (nur Samsung Knox-Geräte) - Gerätefunktionalität | Google zulassen<br>Automatische Synchronisierung | Legen Sie fest, ob Google-Konten und -Apps automatisch synchronisiert werden können. Diese Regel hindert Google Play nicht daran, installierte Apps zu aktualisieren. Benutzer können einige Apps weiterhin manuell synchronisieren, einschließlich Gmail. | Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Persönliches Profil (nur Samsung Knox-Geräte) - Gerätefunktionalität | Zulassen, dass Absturzberichte an Google gesendet werden | Legen Sie fest, ob Benutzer Absturzberichte an Google senden können. | Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Persönliches Profil (nur Samsung Knox-Geräte) - Apps | S Voice zulassen | Legen Sie fest, ob die Verwendung der S Voice-App auf dem Gerät zulässig ist. | Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| Android | Persönliches Profil (nur Samsung Knox-Geräte) - Kennwort | Zwei-Faktor-Authentifizierung erzwingen | Legen Sie fest, ob ein Benutzer die Zwei-Faktor-Authentifizierung für den Zugriff auf das Gerät verwenden muss. Sie können diese Regel beispielsweise verwenden, wenn Sie möchten, dass der Benutzer sich per Fingerabdruck und Kennwort authentifizieren muss. | Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Persönliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Andere Geräteadministratoren zulassen | Legen Sie fest, ob ein Gerät zusätzlich zu BlackBerry UEM Client von anderen Apps, wie MDM-Apps, verwaltet werden kann. Wenn diese Regel nicht ausgewählt ist und andere Apps zur Geräteverwaltung aktiviert werden, bevor die Richtlinie an das Gerät gesendet wird, kann die Richtlinie nicht angewendet werden. | Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Geschäftliche Dateien im persönlichen Profil zulassen | Legen Sie fest, ob ein Benutzer auf einem Gerät Dateien aus dem geschäftlichen Profil in das | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und | Nicht ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | persönliche Profil verschieben kann. | persönlich – vollständige Kontrolle | |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Persönliche Dateien im geschäftlichen Profil zulassen | Legen Sie fest, ob ein Benutzer auf einem Gerät Dateien aus dem persönlichen Profil in das geschäftliche Profil verschieben kann. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Synchronisierung geschäftlicher und persönlicher Daten aktivieren | Legen Sie fest, ob Apps Daten zwischen dem geschäftlichen Profil und dem persönlichen Profil synchronisieren können. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Persönliche Kontakte im geschäftlichen Profil zulassen | Legen Sie fest, ob persönliche Kontaktdaten aus der Kontakt-App in das geschäftliche Profil importiert werden dürfen. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Geschäftskontakte im persönlichen Profil zulassen | Legen Sie fest, ob die Kontakt-App geschäftliche Kontaktdaten aus dem geschäftlichen Profil in das persönliche Profil exportieren darf. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Persönliche Kalenderdaten im geschäftlichen Profil zulassen | Legen Sie fest, ob persönliche Kontaktdaten aus der Kalender-App in das geschäftliche Profil importiert werden dürfen. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Geschäftliche Kalenderdaten im persönlichen Profil zulassen | Legen Sie fest, ob die Kalender-App geschäftliche Kalenderdaten aus dem geschäftlichen Profil in das persönliche Profil exportieren darf. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Änderung der Einstellung „Detaillierte Benachrichtigungen anzeigen“ durch Benutzer zulassen | Legen Sie fest, ob Benutzer die Einstellung „Detaillierte Benachrichtigungen anzeigen“ auf einem Gerät ändern können. Diese Einstellung bestimmt, ob auf einem Gerät Informationen über geschäftliche Benachrichtigungen im persönlichen Profil verkürzt angezeigt werden sollen. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Apps dürfen auf externen Speicher zugreifen | Legen Sie die Paket-IDs von Apps im geschäftlichen Profil fest, die Lese- oder Schreibrechte | Geschäftlich und persönlich – Privatsphäre des Benutzers, Nur geschäftlicher Bereich, | |

| | | | | | |
|---|---|---|---|---|---|
| | | | für die SD-Karte haben. | Geschäftlich und persönlich – vollständige Kontrolle | |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Sicherheit und Datenschutz | Andere Geräteadministratoren zulassen | Legen Sie fest, ob ein Gerät zusätzlich zu BlackBerry UEM Client von anderen Apps, wie MDM-Apps, verwaltet werden kann. Wenn diese Regel nicht ausgewählt ist und andere Apps zur Geräteverwaltung aktiviert werden, bevor die Richtlinie an das Gerät gesendet wird, kann die Richtlinie nicht angewendet werden. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Gerätefunktionalität | Zulassen, dass Absturzberichte an Google gesendet werden | Legen Sie fest, ob Benutzer Absturzberichte an Google senden können. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Gerätefunktionalität | Kamera zulassen | Legen Sie fest, ob der Benutzer die Kamera im geschäftlichen Profil verwenden darf. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – | Ausgewählt |

| | | | | | |
|---|---|---|---|---|---|
| | | | | vollständige Kontrolle | |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Apps | S Voice zulassen | Legen Sie fest, ob die Verwendung der S Voice-App auf dem Gerät zulässig ist. | Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Kennwort | Zwei-Faktor-Authentifizierung erzwingen | Legen Sie fest, ob ein Benutzer die Zwei-Faktor-Authentifizierung für den Zugriff auf das geschäftliche Profil verwenden muss. Sie können diese Regel beispielsweise verwenden, wenn Sie möchten, dass der Benutzer sich per Fingerabdruck und Kennwort authentifizieren muss. | Geschäftlich und persönlich – Privatsphäre des Benutzers, Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle | Nicht ausgewählt |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Kennwort | Maximallänge für Zeichenfolge | Legen Sie die maximale Länge der Zeichenfolge fest, die im Kennwort des geschäftlichen Profils zulässig ist. Gilt nur, wenn die Qualität des Kennworts für das geschäftliche Profil alphabetisch, alphanumerisch | Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – Privatsphäre des Benutzers | |

| | | | | | |
|---|---|---|---|---|---|
| | | | oder komplex ist. | | |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Kennwort | Maximale Länge einer Zahlenfolge | Legen Sie die maximale Länge der Zahlenfolge fest, die im Kennwort des geschäftlichen Profils zulässig ist. Gilt nur, wenn die Qualität des Kennworts für das geschäftliche Profil numerisch, alphanumerisch oder komplex ist. | Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – Privatsphäre des Benutzers | |
| Android | Geschäftliches Profil (nur Samsung Knox-Geräte) - Kennwort | Mindestanzahl geänderter Zeichen für neue Kennwörter des geschäftlichen Profils | Legen Sie die Mindestanzahl geänderter Zeichen fest, die ein neues Kennwort im Vergleich zu einem vorherigen Kennwort enthalten muss. | Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – Privatsphäre des Benutzers | |

# Neuerungen in BlackBerry UEM Cloud

**iOS**

- **Fehlermeldung zu Aktualisierung von Apple DEP**:Wenn Sie die aktualisierten Geschäftsbedingungen für Apple Business Manager noch nicht akzeptiert haben, erhalten Sie eine Fehlermeldung per E-Mail.
- **Manuelle Synchronisierung der Apple DEP-Konten mit Apple Business Manager**: Sie können Apple DEP-Konten in BlackBerry UEM manuell synchronisieren, um die Gerätekonnektivität zu gewährleisten.
- **Aktualisierung der Ereignisbenachrichtigung**: Die Ereignisbenachrichtigung über den Zustand der Apple DEP-Verbindung enthält jetzt Details für den Kommunikationsstatus, den Betriebsmodus und die Uhrzeit der letzten Synchronisierung.
- **Aktivierungsprofil für Apple DEP-Geräte festlegen**: Für jedes in Apple DEP registrierte Gerät können Sie nun das Aktivierungsprofil angeben, das Sie ihm zuweisen möchten. Wenn ein Benutzer z. B. über mehrere iOS-Geräte verfügt, die unterschiedliche Aktivierungsarten erfordern, können Sie das Aktivierungsprofil für die einzelnen Geräte festlegen. Bei der Aktivierung von iOS-Geräten hat das dem Gerät zugewiesene Aktivierungsprofil Vorrang vor dem Aktivierungsprofil, das dem Benutzerkonto zugewiesen ist.
- **Benutzer Apple DEP-Gerätenummern direkt zuweisen**: Mit BlackBerry UEM können Sie jetzt Benutzer einer Apple DEP-Geräteseriennummern vor der Aktivierung des Geräts direkt zuweisen. Wenn der Benutzer einer Geräteseriennummer in der BlackBerry UEM-Verwaltungskonsole zugeordnet wird, wird er während der Geräteaktivierung nicht zur Eingabe eines Benutzernamens oder Passworts aufgefordert.
- **Aktualisieren von iOS auf eine bestimmte Versionsnummer**: Auf der Registerkarte „Gerät“ können Sie die Softwareversion auf einem überwachten iOS-Gerät auf eine bestimmte Versionsnummer aktualisieren. Sie können diese Funktion verwenden, um das Gerätebetriebssystem auf eine Version zu aktualisieren, die von der IT-Abteilung Ihres Unternehmens zertifiziert wurde.
- **Unterstützung für SSO-Erweiterung unter iOS 13**: Die SSO-Erweiterung für iOS 13 und iPadOS 13 ermöglicht es Benutzern, sich einmal zu authentifizieren und sich dann automatisch bei Domänen und Webservices innerhalb des Unternehmensnetzwerks anzumelden. Sie können ein SSO-Erweiterungsprofil in BlackBerry UEM für Geräte mit iOS (oder iPadOS) 13 konfigurieren.
- **Verbesserter Aktivierungsprozess**: Der BlackBerry UEM Client für iOS wurde mit Sicherheitsmerkmalen aktualisiert, um die Fälle zu minimieren, in denen ein Benutzer den Aktivierungsprozess von Anfang an aufgrund einer Unterbrechung während der Geräteaktivierung neu starten muss (z. B. wenn der Benutzer während der Aktivierung einen Anruf erhält). Wenn der Benutzer zu UEM Client zurückkehrt, kann er nun die Aktivierung vom letzten Schritt an fortsetzen.
- **Neue Aktivierungsart für iOS- und iPadOS 13.1-Geräte**: Eine neue Aktivierungsart „Benutzerdatenschutz - Benutzerregistrierung“ ist nun für nicht überwachte iOS-Geräte mit iOS oder iPadOS 13.1 und höher verfügbar. Die Aktivierungsart trägt dazu bei, die Privatsphäre des Benutzers zu wahren, während die geschäftlichen Daten getrennt und geschützt bleiben. Administratoren können geschäftliche Daten verwalten (z. B. geschäftliche Daten löschen), ohne dass Auswirkungen auf persönliche Daten erfolgen. Um ein Gerät mit dieser Aktivierungsart zu aktivieren, können Benutzer einfach den in der Aktivierungs-E-Mail erhaltenen QR Code mit der nativen Kamera-App scannen und das MDM-Profil manuell auf das Gerät herunterladen und installieren. Um das Gerät zu aktivieren, meldet sich der Benutzer bei seinem verwalteten Apple ID-Konto an. Administratoren können zudem den BlackBerry UEM Client zuweisen, um Benutzern die einfache Aktivierung anderer BlackBerry Dynamics-Apps, das Importieren von Zertifikaten, die Verwendung von 2FA-Funktionen und die Verwendung von CylancePROTECT Mobile for BlackBerry UEM zu ermöglichen und deren Konformitätsstatus zu prüfen.
- **Unterstützung für iOS 13-Funktionen**: BlackBerry UEM unterstützt die neuen Funktionen in iOS 13. Die Unterstützung umfasst drei neue IT-Richtlinienregeln, Unterstützung für WPA-3 Personal- und WPA-3 Enterprise Wi-Fi-Sicherheit sowie neue Profileinstellungen für E-Mail, VPN-Profil und App-Sperrmodus.

### Android

- **Profil für den werkseitigen Rücksetzschutz**: Sie können für mehrere Google-Konten ein Profil für den werkseitigen Rücksetzschutz festlegen.
- **Verbesserte Benutzererfahrung bei der Android Enterprise-Geräteaktivierung**: Die Anzahl der erforderlichen Schritte zur Aktivierung von Android Enterprise-Geräten wurde reduziert. Benutzer können jetzt auf ein Kontrollkästchen tippen, wenn sie ihren Benutzernamen eingeben, um die Lizenzvereinbarung zu akzeptieren. Zusätzliche Benachrichtigungen wurden hinzugefügt, um den Fortschritt der App-Installation anzuzeigen. Es wurden zusätzliche Meldungen hinzugefügt, die die für UEM Client erforderlichen Berechtigungen beschreiben.
- **Aktualisierte Aktivierungsfehlermeldungen**: Wenn die Aktivierung auf einem Android-Gerät nicht erfolgreich war, wird eine neue oder aktualisierte Fehlermeldung angezeigt, die erklärt, warum das Gerät nicht ordnungsgemäß aktiviert wurde. Dadurch können Benutzer und IT-Mitarbeiter das Problem diagnostizieren und beheben.
- **Verwenden von OEMConfig-Apps von Android-Geräteherstellern zum Verwalten von Gerätefunktionen**: BlackBerry UEM unterstützt die Verwendung von OEMConfig-Apps von Geräteherstellern (z. B. Samsung Knox Service Plugin) zur Verwaltung von herstellerspezifischen APIs auf Geräten. Mit dem Samsung Knox Service-Plug-in können Sie neue Samsung-Gerätefunktionen verwalten, sobald Samsung Geräte oder Apps aktualisiert, anstatt bis zur nächsten UEM-Aktualisierung auf neue Profileinstellungen und IT-Richtlinienregeln zu warten.
- **Feedback von Android-Apps mit App-Konfigurationen anzeigen**: BlackBerry UEM empfängt und zeigt Fehler- und Informationsfeedback von Android-Apps an, die über eine App-Konfiguration verfügen und für Feedback entwickelt wurden.
- **Einfaches Hinzufügen geschäftlicher Apps für Android Enterprise-Geräte zu Google Play**: Zugriff auf die aktualisierte Google Play-Benutzeroberfläche von BlackBerry UEM aus, um private Apps und Web-Apps (Verknüpfungen zu Webseiten) zu Google Play im geschäftlichen Profil auf Android Enterprise-Geräten hinzuzufügen.
- **Unterstützung für COSU-Geräte (unternehmenseigene Einzweckgeräte) für Android Enterprise**: BlackBerry UEM unterstützt nun unternehmenseigene Einzweckgeräte für Android Enterprise ab Version 9.0. Ein Gerät mit COSU-Konfiguration ist für eine bestimmte Reihe von Anwendungen gesperrt bzw. auf eine bestimmte Funktion beschränkt.
- **Fehlerbericht anfordern**: Sie können jetzt einen Befehl von Android Enterprise an ein BlackBerry UEM-Gerät senden, um die Client-Protokolle anzufordern. Für die folgenden Aktivierungsarten kann ein Fehlerbericht angefordert werden:
  - Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)
  - Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil)
- **Steuern von Laufzeitberechtigungen für Android-Apps**: Wenn Sie eine Android-App in BlackBerry UEM hinzufügen, können Sie Laufzeitberechtigungen für die App festlegen. Sie können für die jeweilige für die App aufgeführte Berechtigung Berechtigungen erteilen, Berechtigungen verweigern oder eine App-Berechtigungsrichtlinie verwenden.
- **Client-Downloadverzeichnis mit QR Code senden**: Sie können das Downloadverzeichnis des UEM Client für die Aktivierungsarten „Nur geschäftlicher Bereich“ (vollständig verwaltetes Android Enterprise-Gerät) und „Geschäftlich und persönlich – vollständige Kontrolle“ (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil) definieren. Das Verzeichnis wird im QR Code gesendet.
- **Datumsbereich für OS-Aktualisierungen**: Für Android Enterprise-Geräte mit den Aktivierungsarten „Nur geschäftlicher Bereich“ und „Geschäftlich und persönlich – vollständige Kontrolle“ können Sie jetzt einen Datumsbereich angeben, in dem keine Betriebssystemaktualisierung stattfinden sollen.
- **Beim Löschen des geschäftlichen Profils wird eine Meldung angezeigt**: Wenn Sie den Befehl „Nur Geschäftsdaten löschen“ für Android Enterprise-Geräte mit den Aktivierungsarten „Geschäftlich und persönlich – Benutzerdatenschutz“ verwenden, können Sie einen Grund angeben, der in der Benachrichtigung auf dem Gerät des Benutzers angezeigt wird, um zu erklären, warum das geschäftliche Profil gelöscht wurde.

- **Wenn das geschäftliche Profil aufgrund eines Konformitätsverstoßes gelöscht wird, wird eine Meldung angezeigt**: Wenn das geschäftliche Profil aufgrund eines Konformitätsverstoßes von einem Android Enterprise-Gerät mit der Aktivierungsart „Geschäftlich und persönlich – Benutzerdatenschutz“ gelöscht wird, beschreibt die Benachrichtigung auf dem Gerät jetzt, gegen welche Konformitätsregel verstoßen wurde.
- **Neustart des Geräts erzwingen**: Sie können jetzt den Befehl „Gerät neu starten“ verwenden, um Android Enterprise-Geräte mit der Aktivierungsart „Nur geschäftlicher Bereich“ und „Geschäftlich und persönlich – vollständige Kontrolle“ neu zu starten.
- **Verbesserte sichere Tunnelverbindung für Android-Geräte**: Wenn ein Android-Gerät in den Ruhemodus wechselt, wird die BlackBerry Secure Connect Plus-Verbindung nun zuverlässiger aufrechterhalten.
- **Standardprofil für Gerätedienstanforderungen und Aktualisierungen für geschäftliche Apps**: Es ist jetzt ein Standardprofil für Gerätedienstanforderungen verfügbar, das Benutzerkonten zugewiesen werden kann, denen noch kein Profil für Gerätedienstanforderungen zugewiesen ist. Das Standardprofil ist nur für Android-Geräte konfiguriert und wird mit aktivierter Option „Updatezeitraum für im Vordergrund laufende Apps aktivieren“ ausgeliefert, mit der geschäftliche Apps von Google Play während des Zeitraums automatisch aktualisiert werden können. Standardmäßig ist der Start der App-Aktualisierungen über Wi-Fi um 02:00 Uhr (lokale Zeitzone des Geräts) geplant. Nach 4 Stunden ist der Aktualisierungszeitraum beendet.
- **Android Enterprise-Geräte auf eine einzige App beschränken**: Das App-Sperrmodus-Profil wird jetzt für Geräte mit Android 9 oder höher unterstützt, die die Aktivierungsart „Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)“ aufweisen. Sie können jetzt das Profil verwenden, um Android Enterprise-Geräte auf die von Ihnen angegebenen Apps zu beschränken und das Gerät optional auf eine einzelne App zu beschränken. Wenn Sie das Gerät auf eine einzelne App beschränken, kann die App bei Bedarf auf die anderen Apps zugreifen, die Sie im Profil angegeben haben. Benutzer kehren jedoch immer zu der App zurück, auf die das Gerät beschränkt ist.

#### Samsung Knox

- **Unterstützung für Samsung Knox DualDAR**: Geräte, die Samsung Knox DualDAR-Verschlüsselung unterstützen, können Knox Workspace-Daten nun mit zwei Verschlüsselungsschichten sichern. Wenn der Benutzer das Gerät nicht verwendet, sind alle Daten in Knox Workspace gesperrt und können nicht von im Hintergrund ausgeführten Apps aufgerufen werden. Im Aktivierungsprofil können Sie angeben, ob Sie die standardmäßige DualDAR-App oder eine interne App zum Verschlüsseln des Arbeitsbereichs verwenden möchten. Im Geräteprofil können Sie das Zeitlimit für die Datensperre festlegen, nach dem der Benutzer sich sowohl bei dem Gerät als auch beim Arbeitsbereich authentifizieren muss, um wieder auf geschäftliche Daten zuzugreifen. Außerdem können Sie Apps festlegen, die auf geschäftliche Daten zugreifen dürfen, selbst wenn geschäftliche Daten gesperrt sind.

  Die Samsung Knox DualDAR-Verschlüsselung wird auf Geräten mit Samsung Knox ab Version 3.3 für neue Aktivierungen mit der Premium-Aktivierungsart „Geschäftlich und persönlich - vollständige Kontrolle“ (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil) unterstützt.
- **Verbesserte Unterstützung für Knox Platform for Enterprise-Geräte**: Samsung Knox-IT-Richtlinien wurden für Geräte hinzugefügt, die Knox Platform for Enterprise unterstützen. Diese Richtlinien werden je nach ausgewählter Android Enterprise-Aktivierungsart auf das Gerät, den persönlichen Bereich oder den geschäftlichen Bereich auf dem Gerät angewendet. Außerdem wurde Unterstützung für natives Samsung-VPN und E-Mail hinzugefügt, die Möglichkeit, Apps im persönlichen Bereich einzuschränken und den geschäftlichen Bereich per Fernzugriff zu sperren. Um Knox Platform for Enterprise-Funktionen verwenden zu können, ist auf dem Knox-Gerät Android 8 oder höher sowie eine der Android Enterprise-Aktivierungsarten mit Premium-Option erforderlich.

#### Windows

- **BitLocker-Verschlüsselungsrichtlinien für Windows 10-Geräte**: Mehrere IT-Richtlinien, die die Verwendung von BitLocker Drive Encryption unterstützen, wurden UEM für Windows 10-Geräte hinzugefügt, die eine

Verschlüsselung erfordern. Bei entsprechender Konfiguration werden Benutzer von den Geräten aufgefordert, Daten mit BitLocker auf ihren Betriebssystemlaufwerken, Festplattenlaufwerken und Wechseldatenträgern zu verschlüsseln. Sie können die Verschlüsselungsstärke, die zusätzlichen Authentifizierungsanforderungen und die PIN-Optionen für Geräte konfigurieren, die über ein Trusted Platform Module verfügen, sowie die Wiederherstellungsoptionen, die Sie zulassen möchten (z. B. wenn das Gerät eines Benutzers gesperrt ist).

#### Software-Unterstützung

Die folgende Software wird von BlackBerry UEM nicht mehr unterstützt:

- iOS Version 11: (weitere Informationen finden Sie unter support.blackberry.com im Artikel KB57538)
- Android OS Version 6 (weitere Informationen finden Sie unter support.blackberry.com im Artikel KB57539)
- BlackBerry 10 OS (weitere Informationen finden Sie unter Übersicht zum Lebenszyklus der BlackBerry-Software)

#### Verwaltungskonsole

- **Konformitätsprofilaktualisierungen**: In einem Konformitätsprofil können Sie jetzt die Erzwingungsaktion für BlackBerry Dynamics-Apps auf Überwachen und Protokollieren setzen. „Überwachen und Protokollieren“ ist jetzt die Standardeinstellung für Konformitätsprofile. Die Standardoption für die Aktion „Aktion bei Ablauf des Aufforderungsintervalls“ ist ebenfalls „Überwachen und Protokollieren“.
- **Verbesserungen bei der Gerätefilterung**: Sie können Geräte jetzt nach Modellnummer filtern. Sie können jetzt beispielsweise nach unterschiedlichen Samsung Galaxy-Gerätemodellen wie Samsung A5 SM-A520F und Samsung A5 SM-A510F filtern. Auf diese Weise können Administratoren Richtlinien, Profile und Gruppenstatus auf mehrere Geräte eines bestimmten Modells anwenden.
- **App-Konfiguration**: Wenn Sie eine neue Version einer internen App zu BlackBerry UEM hinzufügen, wird die App-Konfiguration automatisch von der älteren Version der internen App in die neue Version kopiert.
- **Aktualisierung der Ereignisbenachrichtigung**: Die Ereignisbenachrichtigung „Aktualisierung von Metadaten“ wurde verbessert und zeigt nun den vollständigen Namen des Gerätehardwareanbieters an.
- **Überschreiben von BlackBerry Dynamics-Konnektivitätsprofilen auf App-Basis**: Sie können jetzt ein BlackBerry Dynamics-Konnektivitätsprofil angeben, das mit der jeweiligen BlackBerry Dynamics-App in BlackBerry UEM verknüpft werden soll. Wenn ein Profil einer App zugewiesen wird, hat dieses Profil Vorrang vor dem Profil, das dem Benutzer dieser App zugewiesen wurde.
- **App-Verknüpfungsfilter**: Mit einem neuen Filter auf der App-Seite der UEM-Verwaltungskonsole können Sie nach App-Verknüpfungen suchen.
- **Dedizierte Gerätegruppen**: BlackBerry UEM enthält eine neue Menüoption „Dedizierte Geräte“. Sie können freigegebene Gerätegruppen und öffentliche Gerätegruppen im Menü „Dedizierte Geräte“ anzeigen, hinzufügen, bearbeiten und löschen. Öffentliche Gerätegruppen werden zur Verwaltung von zweckbestimmten Geräten verwendet, die nicht bestimmten Benutzern zugewiesen sind. Freigegebene Gerätegruppen werden zur Verwaltung von Geräten verwendet, die von mehreren Benutzern ausgecheckt werden können. Zuvor waren freigegebene Gerätegruppen unter dem Menüpunkt „Benutzer“ zu finden.
- **Microsoft Azure Einzelmandanten-Anwendungsregistrierung**: Wenn Sie eine Verbindung zu Microsoft Azure Active Directory Connect hinzufügen oder bearbeiten, können Sie die Einzelmandanten-Anwendungsregistrierung aktivieren.
- **Registrierung mithilfe von Geräte-IDs einschränken**: Auf der Seite „Standardeinstellungen für die Aktivierung“ können Sie eine Liste eindeutiger Gerätekennungen importieren und exportieren, um zu beschränken, welche Geräte bei BlackBerry UEM registriert werden können. Sie können festlegen, ob BlackBerry UEM die Aktivierung nach Geräte-ID in den folgenden Aktivierungsarten eingeschränkt werden kann:

  **Android**

  - Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)
  - Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät)

**iOS**

- MDM-Steuerelemente

- **SCEP-Profilaktualisierung**: Mit einer neuen Schaltfläche im SCEP-Profil können Sie die Verbindung zwischen der BlackBerry UEM Cloud-Instanz und dem SCEP-Server über den BlackBerry Connectivity Node testen. Die Schaltfläche ist nur aktiviert, wenn BlackBerry Connectivity Node für die Weiterleitung von SCEP-Anrufen konfiguriert ist. Sie können BlackBerry Connectivity Node verwenden, um eine BlackBerry UEM Cloud -Instanz mit einem SCEP-Server innerhalb der Firewall zu verbinden.
- **Google-Benachrichtigungen**: Sie können Google-Benachrichtigungen für BlackBerry UEM Cloud aktivieren. Sie müssen die Verbindung zu Ihrer Google-Domäne wiederherstellen, um eine eindeutige Identität für Ihren Mandanten zu erstellen, und dann die Geräte erneut aktivieren.
- **BlackBerry Online Account-Anmeldeinformationen**: Administratoren können jetzt Benutzer in BlackBerry UEM Cloud erstellen, die ihre BlackBerry Online Account-Anmeldeinformationen für die Anmeldung verwenden können.

#### BlackBerry Dynamics

- **BlackBerry Dynamics-Proxy-Einstellungen mit PAC-Datei konfigurieren**: Sie können jetzt eine PAC-Datei verwenden, um HTTP-Proxy-Einstellungen für Verbindungen des App-Datenverkehrs zu BlackBerry Dynamics NOC konfigurieren. PAC-Dateien werden nur für Apps unterstützt, die BlackBerry Dynamics SDK ab Version 7.0 verwenden.
- **TLS v1.2**: Für BlackBerry Dynamics-Apps ist standardmäßig nur noch TLS v1.2 für eine sichere Kommunikation zulässig. TLSv1- und v1.1-Verschlüsselungen müssen manuell konfiguriert werden.

#### BlackBerry Enterprise Mobility Server

- **Verbesserungen bei vertrauenswürdige Verbindung zu Microsoft Exchange Server**: Sie können jetzt einzelne CA- und Zwischenzertifikate aus dem BEMS-Zertifikatspeicher über die BlackBerry UEM-Konsole importieren und entfernen. Auf diese Weise können Administratoren selbstsignierte und benutzerdefinierte Zertifikate der Zertifizierungsstelle ggf. importieren und ersetzen, um die vertrauenswürdige Verbindung zwischen BEMS Cloud und dem Microsoft Exchange Server herzustellen.
- **Verbesserungen bei E-Mail-Benachrichtigungen**: Wenn Sie die Verbindung eines Benutzerprofils zu Microsoft Exchange Server oder Microsoft Office 365 für E-Mail-Benachrichtigungen (Einstellungen > BlackBerry Dynamics > E-Mail-Benachrichtigungen) in der Umgebung testen, enthält BEMS Cloud eindeutige Meldungen zum Fehlschlagen des Tests (z. B. Ungültige Anmeldeinformationen: überprüfen Sie, ob die Microsoft Exchange-Anmeldeinformationen korrekt sind).
- **BlackBerry Connectivity Node-Konfigurationsverbesserungen**: Administratoren können angeben, dass BEMS Cloud die interne Microsoft Exchange Web Services-URL für E-Mail-Benachrichtigungen von BEMS Cloud verwendet (Einstellungen > BlackBerry Dynamics > E-Mail-Benachrichtigungen), wenn die Umgebung so konfiguriert ist, dass sie eine interne URL für den Zugriff auf und die Kommunikation mit einem lokalen Microsoft Exchange Server verwendet.

#### Neue IT-Richtlinienregeln

- **APN-Profil**: Sie können APN-Profile (Access Point Name) verwenden, um APNs für Betreiber an die Android-Geräte von Benutzern zu senden. Wenn Sie ein Gerät zwingen möchten, einen APN zu verwenden, der von einem APN-Profil an das Gerät gesendet wird, können Sie die IT-Richtlinienregel „Gerät zur Verwendung der APN-Profileinstellungen zwingen“ in den IT-Richtlinienregeln von Android Global IT verwenden.
- **Zertifikat ausblenden**: Für Zertifikate, die mit Push an Android Enterprise-Geräte mit Android 9.0 und höher gesendet werden, können Sie mit SCEP, freigegebenen Zertifikaten und Profilen für

Benutzeranmeldeinformationen jetzt das Zertifikat vor Benutzern verbergen, um dessen Verwendung für nicht beabsichtigte Zwecke zu verhindern.

| Gerätetyp | Name | Beschreibung | Aktivierungsarten |
|---|---|---|---|
| iOS | Verwendung von USB durch Dateien-App zulassen (nur unter Aufsicht) | Legen Sie fest, ob die Dateien-App über eine USB-Verbindung auf Dateien zugreifen kann. | MDM-Steuerelemente |
| iOS | Verbindung zu Netzlaufwerken über Dateien-App zulassen (nur unter Aufsicht) | Legen Sie fest, ob die Dateien-App auf Dateien zugreifen kann, die auf einem Netzlaufwerk gespeichert sind. | MDM-Steuerelemente |
| iOS | Aktivierung von Wi-Fi erzwingen (nur unter Aufsicht) | Legen Sie fest, ob Wi-Fi auf dem Gerät immer aktiviert ist. Wenn diese Regel ausgewählt ist, können Benutzer Wi-Fi nicht über die Geräteeinstellungen oder das Control Center ausschalten, und Wi-Fi wird im Flugmodus nicht deaktiviert. | MDM-Steuerelemente |
| iOS | Verbindung zu Netzlaufwerken über Dateien-App zulassen (nur unter Aufsicht) | Legen Sie fest, ob die Dateien-App auf Dateien zugreifen kann, die auf einem Netzlaufwerk gespeichert sind. | MDM-Steuerelemente |
| macOS | Bluetooth aktivieren | Legen Sie fest, ob Bluetooth aktiviert oder deaktiviert ist, wenn die Richtlinie an das Gerät gesendet wird. Unabhängig von der Einstellung für diese Regel können Benutzer die Bluetooth-Einstellung auf ihrem Gerät jederzeit ändern. | MDM-Steuerelemente |
| Android Global (alle Android-Geräte) | Timeout bei sekundärer Authentifizierung | Legen Sie fest, wie lange der Benutzer maximal sekundäre Authentifizierungsmethoden (z. B. einen Fingerabdruck) verwenden kann, | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich |

| | | | |
|---|---|---|---|
| | | bevor er das Gerät mit einer starken Authentifizierungsmethode, z. B. einem Kennwort, entsperren muss. Der Höchstwert beträgt 72 Stunden. Wenn der Wert auf 0 gesetzt ist, wird kein Timeout-Wert an das Gerät gesendet. Diese Regel wird nur wirksam, wenn die Regel „Kennwortanforderungen“ auf eine andere Einstellung als „Nicht angegeben“ festgelegt ist. | und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (alle Android-Geräte) | Installation von Apps zulassen, die nicht von Google Play stammen | Legen Sie fest, ob Benutzer Apps aus anderen Quellen als Google Play (unbekannte Quellen) global auf dem Gerät für alle Benutzer installieren können. Wenn Sie die Installation von Nicht-Google Play-Apps mit dieser Regel nicht zulassen, werden die Einstellungen für dieselbe Regel in persönlichen und geschäftlichen Profilen ignoriert. Wenn diese Regel ausgewählt ist, können Sie die Installation von Apps, die nicht von Google Play stammen, nur im geschäftlichen Profil oder nur im persönlichen Profil als nicht zulässig festlegen. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | USB-Fehlerbehebung aktivieren | Legen Sie fest, ob die Fehlerbehebung über eine USB-Verbindung verfügbar ist. Wenn diese Regel nicht ausgewählt ist, wird die Fehlerbehebung mit dem Dalvik Debug | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – |

| | | | |
|---|---|---|---|
| | | Monitor Service (DDMS) ebenfalls blockiert. Diese Regel ist nur verfügbar, wenn die Regel „Entwicklermodus zulassen“ ausgewählt ist. | vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Ausgehende SMS zulassen | Legen Sie fest, ob ein Gerät SMS-Nachrichten senden kann. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Eingehende SMS zulassen | Legen Sie fest, ob ein Gerät SMS-Nachrichten empfangen kann. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Interne Speicherverschlüsselung erforderlich | Legen Sie fest, ob der Benutzer dazu aufgefordert wird, den Gerätespeicher und die interne SD-Karte des Geräts zu verschlüsseln. Wenn diese Regel ausgewählt ist, können keine Remote-Administrationsbefehl wie das Ändern des Kennworts oder das Bereinigen des Geräts ausgeführt werden, es sei denn, das Gerät wird bereits ausgeführt und der Benutzer kann sich anmelden (oder ist angemeldet). Für diese Regel muss die Regel „Kennwortanforderungen“ mindestens den Wert „Alphanumerisch“ | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| | | aufweisen. Der Gerätespeicher und die interne SD-Karte müssen vom Benutzer vor einer Aktivierung verschlüsselt werden, damit die Aktivierung abgeschlossen werden kann. | |
| Android Global (nur Samsung Knox-Geräte) | Benutzern die Änderung des Pseudostandorts gestatten | Legen Sie fest, ob ein Benutzer die Angabe eines falschen GPS-Standorts auf dem Gerät aktivieren oder deaktivieren kann. Ist diese Regel ausgewählt, können die Angaben von Längen- und Breitengrad des Geräts geändert werden, und GPS-Apps zeigen anstatt der tatsächlichen Koordinaten falsche Koordinaten an. Diese Regel ist nur verfügbar, wenn die Regel „Entwicklermodus zulassen“ ausgewählt ist. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Maximale Länge einer Zahlenfolge | Legen Sie die maximale Länge der Zahlenfolge fest, die im Gerätekennwort zulässig ist. Gilt nur, wenn die Qualität des Gerätekennworts numerisch, alphanumerisch oder komplex ist. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Mindestanzahl geänderter Zeichen für neue Gerätekennwörter | Legen Sie die Mindestanzahl geänderter Zeichen fest, die ein neues Kennwort im Vergleich zu einem vorherigen Kennwort enthalten muss. Knox berechnet den Unterschied zwischen den beiden Kennwörtern anhand | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| | | des Levenshtein-Algorithmus. Zulässige Zeichen sind Zahlen, Buchstaben oder Symbole. Gemäß Levenshtein-Algorithmus unterscheiden sich Zeichenfolgen wie "test" und "best" durch ein Element voneinander. "Test" und "toad" unterscheiden sich durch drei Elemente voneinander. "Test" und "est" unterscheiden sich durch ein Element voneinander. Wenn 0 eingestellt ist, gelten keine Einschränkungen. | |
| Android Global (nur Samsung Knox-Geräte) | Sichtbarkeit des Gerätekennworts zulassen | Legen Sie fest, ob das Gerätekennwort bei der Eingabe sichtbar sein soll. Wenn diese Regel nicht ausgewählt ist, kann die Sichtbarkeitseinstellung von Benutzern oder Apps nicht geändert werden. | Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Sperrbildschirmmeldung anfordern | Legen Sie fest, ob eine Meldung angezeigt werden soll, wenn das Gerät gesperrt wird. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer eine Meldung für den Sperrbildschirm auswählen. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Sperrbildschirmmeldung | Legen Sie den Text fest, der auf dem Bildschirm beim Sperren des Geräts angezeigt werden soll. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| Android Global (nur Samsung Knox-Geräte) | Maximallänge für Zeichenfolge | Legen Sie die maximale Länge der Zeichenfolge fest, die im Gerätekennwort zulässig ist. Gilt nur, wenn die Qualität des Gerätekennworts alphabetisch, alphanumerisch oder komplex ist. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Telefon zulassen | Legen Sie fest, ob ein Benutzer das Telefon verwenden kann. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer mit dem Gerät nur Notrufe tätigen. Alle anderen Anrufe werden gesperrt. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Datums- und Uhrzeitänderungen zulassen | Legen Sie fest, ob Benutzer die Einstellung für Datum und Uhrzeit auf einem Gerät ändern können. | Nur geschäftlicher Bereich (Premium), Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Automatische Zeitsynchronisierung erzwingen | Legen Sie fest, ob das Gerät mithilfe von NITZ das Datum und die Uhrzeit automatisch abrufen kann. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer auswählen, ob das Gerät Datum und Uhrzeit automatisch synchronisiert. | Nur geschäftlicher Bereich (Premium), Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Natives Samsung VPN zulassen | Legen Sie fest, ob ein Benutzer die systemeigene VPN-Funktionalität nutzen kann. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer keine VPN-Sitzung | Nur geschäftlicher Bereich (Premium), Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – |

| | | | |
|---|---|---|---|
| | | öffnen oder auf die VPN-Einstellungen in der App „Einstellungen“ zugreifen. | vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | WAP-Push beim Roaming zulassen | Legen Sie fest, ob ein Gerät beim Roaming WAP-Push-Nachrichten empfangen kann. Wenn diese Regel nicht ausgewählt ist, kann das Gerät beim Roaming keine MMS-Nachrichten empfangen. Der Benutzer kann diese Einstellung nicht auf dem Gerät ändern. Diese Regel gilt nur, wenn das Gerät sich im Roaming-Modus befindet. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Automatische Synchronisierung beim Roaming zulassen | Legen Sie fest, ob das Gerät während des Roamings automatisch Daten synchronisieren kann. Wenn diese Regel nicht ausgewählt ist, kann ein Gerät im Roaming-Modus Daten nur synchronisieren, wenn der Benutzer auf ein Konto zugreift. Der Benutzer kann diese Einstellung nicht auf dem Gerät ändern. Diese Einstellung gilt nur, wenn sich das Gerät im Roaming-Modus befindet. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Anrufe beim Roaming zulassen | Legen Sie fest, ob ein Gerät beim Roaming Sprachanrufe tätigen oder empfangen kann. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | SD-Karte zulassen | Legen Sie fest, ob ein Gerät auf eine SD- | Nur geschäftlicher Bereich, Nur |

| | | | |
|---|---|---|---|
| | | Karte zugreifen kann. Wenn diese Regel nicht ausgewählt ist, wird der Lese- und Schreibzugriff auf die SD-Karte gesperrt. | geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Daten im Mobilfunknetz zulassen | Legen Sie fest, ob ein Gerät eine Mobilfunknetzverbindung verwenden kann. Wenn diese Regel nicht ausgewählt ist, kann das Gerät die SIM-Datenverbindung nicht verwenden. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Hinzufügen neuer Wi-Fi-Netzwerke durch Benutzer zulassen | Legen Sie fest, ob Benutzer dem Gerät neue Wi-Fi-Profile hinzufügen können. Wenn diese Regel nicht ausgewählt ist, können Benutzer nur die von Ihnen konfigurierten geschäftlichen Wi-Fi-Profile verwenden. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Android zulassen<br>Beam | Legen Sie fest, ob Benutzer Android Beam oder S Beam verwenden können, um Kontaktinformationen, Web-Lesezeichen und andere Daten an Geräte in der Nähe zu senden. Legen Sie fest, ob Benutzer Android Beam oder S Beam verwenden können, um Kontaktinformationen, Web-Lesezeichen und andere Daten an Geräte in der Nähe zu senden. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | Media Transfer Protocol (MTP) zulassen | Legen Sie fest, ob ein Gerät MTP verwenden kann. Da Android die USB-Dateiübertragung nur | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – |

| | | | |
|---|---|---|---|
| | | über MTP unterstützt, können Sie mit dieser Regel alle Arten der Dateiübertragung über USB blockieren. Picture Transfer Protocol (PTP) ist eine Untergruppe von MTP und ist von dieser Regel ebenfalls betroffen. | vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Global (nur Samsung Knox-Geräte) | USB-Hostspeicher zulassen | Legen Sie fest, ob ein Gerät USB-Hostspeicher mittels USB OTG verwenden kann. Ist diese Regel ausgewählt, kann ein Benutzer USB-Sticks (tragbare USB-Speicher), externe Festplatten oder SD Card Reader anschließen, die auf dem Gerät als Speicherlaufwerk genutzt werden können. Ist diese Regel nicht ausgewählt, kann der Benutzer keine externen Speichergeräte installieren. | Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (alle Android-Geräte) | Timeout bei sekundärer Authentifizierung | Legen Sie fest, wie lange der Benutzer maximal sekundäre Authentifizierungsmethoden (z. B. einen Fingerabdruck) verwenden kann, bevor er das Gerät mit einer starken Authentifizierungsmethode, z. B. einem Kennwort, entsperren muss. Der Höchstwert beträgt 72 Stunden. Wenn der Wert auf 0 gesetzt ist, wird kein Timeout-Wert an das Gerät gesendet. Diese Regel wird nur wirksam, wenn die Regel „Kennwortanforderungen“ auf eine andere Einstellung als „Nicht | Geschäftlich und persönlich – Privatsphäre des Benutzers, Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| | | angegeben“ festgelegt ist. | |
| Android Persönliches Profil (nur Samsung Knox-Geräte) | Audioaufnahme zulassen | Legen Sie fest, ob mit einem Gerät Audioaufnahmen gemacht werden können. Wenn diese Regel nicht ausgewählt ist, kann der Benutzer dennoch Anrufe tätigen und Audio-Streaming mit dem Gerätemikrofon nutzen. Die Regel gilt für Telefonanrufe, Spracherkennung und VoIP. Wenn eine App einen Nutzungstyp deklariert und einen anderen Vorgang ausführt, kann diese Regel die App nicht blockieren. Wenn Sie diese Regel deaktivieren, werden alle laufenden Audioaufnahmen unterbrochen. Videoaufnahmen sind weiterhin zulässig, solange kein Audioaufnahmeversuch erfolgt. Diese Regel gilt nur für den persönlichen Bereich. | Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Persönliches Profil (nur Samsung Knox-Geräte) | Videoaufnahme zulassen | Legen Sie fest, ob mit einem Gerät Videoaufnahmen gemacht werden können. Wenn diese Regel nicht ausgewählt ist, ist die Kamera dennoch verfügbar, und der Benutzer kann fotografieren und Video-Streaming nutzen. Wenn diese Regel nicht ausgewählt ist, werden alle laufenden Videoaufnahmen unterbrochen. | Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| Android Persönliches Profil (nur Samsung Knox-Geräte) | Google zulassen<br>Automatische Synchronisierung | Legen Sie fest, ob Google-Konten und -Apps automatisch synchronisiert werden können. Diese Regel hindert Google Play nicht daran, installierte Apps zu aktualisieren. Benutzer können einige Apps weiterhin manuell synchronisieren, einschließlich Gmail. | Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Persönliches Profil (nur Samsung Knox-Geräte) | Zulassen, dass Absturzberichte an Google gesendet werden | Legen Sie fest, ob Benutzer Absturzberichte an Google senden können. | Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Persönliches Profil (nur Samsung Knox-Geräte) | S Voice zulassen | Legen Sie fest, ob die Verwendung der S Voice-App auf dem Gerät zulässig ist. | Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Persönliches Profil (nur Samsung Knox-Geräte) | Zwei-Faktor-Authentifizierung erzwingen | Legen Sie fest, ob ein Benutzer die Zwei-Faktor-Authentifizierung für den Zugriff auf das Gerät verwenden muss. Sie können diese Regel beispielsweise verwenden, wenn Sie möchten, dass der Benutzer sich per Fingerabdruck und Kennwort authentifizieren muss. | Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Persönliches Profil (nur Samsung Knox-Geräte) | Andere Geräteadministratoren zulassen | Legen Sie fest, ob ein Gerät zusätzlich zu BlackBerry UEM Client von anderen Apps, wie MDM-Apps, verwaltet werden kann. Wenn diese Regel nicht ausgewählt ist und andere Apps zur Geräteverwaltung aktiviert werden, bevor die Richtlinie an das Gerät gesendet wird, | Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| | | kann die Richtlinie nicht angewendet werden. | |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Geschäftliche Dateien im persönlichen Profil zulassen | Legen Sie fest, ob ein Benutzer auf einem Gerät Dateien aus dem geschäftlichen Profil in das persönliche Profil verschieben kann. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Persönliche Dateien im geschäftlichen Profil zulassen | Legen Sie fest, ob ein Benutzer auf einem Gerät Dateien aus dem persönlichen Profil in das geschäftliche Profil verschieben kann. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Synchronisierung geschäftlicher und persönlicher Daten aktivieren | Legen Sie fest, ob Apps Daten zwischen dem geschäftlichen Profil und dem persönlichen Profil synchronisieren können. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Persönliche Kontakte im geschäftlichen Profil zulassen | Legen Sie fest, ob persönliche Kontaktdaten aus der Kontakt-App in das geschäftliche Profil importiert werden dürfen. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Geschäftskontakte im persönlichen Profil zulassen | Legen Sie fest, ob die Kontakt-App geschäftliche Kontaktdaten aus dem geschäftlichen Profil in das persönliche Profil exportieren darf. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Persönliche Kalenderdaten im geschäftlichen Profil zulassen | Legen Sie fest, ob persönliche Kontaktdaten aus der Kalender-App in das geschäftliche Profil | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich |

| | | | |
|---|---|---|---|
| | | importiert werden dürfen. | und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Geschäftliche Kalenderdaten im persönlichen Profil zulassen | Legen Sie fest, ob die Kalender-App geschäftliche Kalenderdaten aus dem geschäftlichen Profil in das persönliche Profil exportieren darf. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Änderung der Einstellung „Detaillierte Benachrichtigungen anzeigen“ durch Benutzer zulassen | Legen Sie fest, ob Benutzer die Einstellung „Detaillierte Benachrichtigungen anzeigen“ auf einem Gerät ändern können. Diese Einstellung bestimmt, ob auf einem Gerät Informationen über geschäftliche Benachrichtigungen im persönlichen Profil verkürzt angezeigt werden sollen. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Apps dürfen auf externen Speicher zugreifen | Legen Sie die Paket-IDs von Apps im geschäftlichen Profil fest, die Lese- oder Schreibrechte für die SD-Karte haben. | Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Andere Geräteadministratoren zulassen | Legen Sie fest, ob ein Gerät zusätzlich zu BlackBerry UEM Client von anderen Apps, wie MDM-Apps, verwaltet werden kann. Wenn diese Regel nicht ausgewählt ist und andere Apps zur Geräteverwaltung aktiviert werden, bevor die Richtlinie an das Gerät gesendet wird, | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| | | kann die Richtlinie nicht angewendet werden. | |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Zulassen, dass Absturzberichte an Google gesendet werden | Legen Sie fest, ob Benutzer Absturzberichte an Google senden können. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Nur geschäftlicher Bereich, Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Kamera zulassen | Legen Sie fest, ob der Benutzer die Kamera im geschäftlichen Profil verwenden darf. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | S Voice zulassen | Legen Sie fest, ob die Verwendung der S Voice-App auf dem Gerät zulässig ist. | Nur geschäftlicher Bereich (Premium), Nur geschäftlicher Bereich, Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Zwei-Faktor-Authentifizierung erzwingen | Legen Sie fest, ob ein Benutzer die Zwei-Faktor-Authentifizierung für den Zugriff auf das geschäftliche Profil verwenden muss. Sie können diese Regel beispielsweise verwenden, wenn Sie möchten, dass der Benutzer sich per Fingerabdruck und Kennwort authentifizieren muss. | Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium), Nur geschäftlicher Bereich (Premium), Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Maximallänge für Zeichenfolge | Legen Sie die maximale Länge der Zeichenfolge fest, die im Kennwort | Geschäftlich und persönlich – vollständige Kontrolle |

| | | | |
|---|---|---|---|
| | | des geschäftlichen Profils zulässig ist. Gilt nur, wenn die Qualität des Kennworts für das geschäftliche Profil alphabetisch, alphanumerisch oder komplex ist. | (Premium), Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Maximale Länge einer Zahlenfolge | Legen Sie die maximale Länge der Zahlenfolge fest, die im Kennwort des geschäftlichen Profils zulässig ist. Gilt nur, wenn die Qualität des Kennworts für das geschäftliche Profil numerisch, alphanumerisch oder komplex ist. | Geschäftlich und persönlich – vollständige Kontrolle (Premium), Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium) |
| Geschäftliches Android-Profil (nur Samsung Knox-Geräte) | Mindestanzahl geänderter Zeichen für neue Kennwörter des geschäftlichen Profils | Legen Sie die Mindestanzahl geänderter Zeichen fest, die ein neues Kennwort im Vergleich zu einem vorherigen Kennwort enthalten muss. | Geschäftlich und persönlich – vollständige Kontrolle (Premium), Geschäftlich und persönlich – Privatsphäre des Benutzers (Premium) |
| Android – persönliches Profil (alle Android-Geräte) | Zugelassene System-Apps | Legen Sie die Paket-IDs für die System-Apps fest, die im persönlichen Bereich installiert sind. Wenn Sie Apps aus dieser Liste entfernen, werden die Apps aus dem persönlichen Bereich auf den Geräten der Benutzer gelöscht. | Geschäftlich und persönlich – vollständige Kontrolle, Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
| Android Persönliches Profil (nur Samsung Knox-Geräte) | Andere Geräteadministratoren zulassen | Legen Sie fest, ob ein Gerät zusätzlich zu BlackBerry UEM Client von anderen Apps, wie MDM-Apps, verwaltet werden kann. Wenn diese Regel nicht ausgewählt ist und andere Apps zur Geräteverwaltung aktiviert werden, bevor die Richtlinie an das Gerät gesendet wird, | Geschäftlich und persönlich – vollständige Kontrolle (Premium) |

| | | | |
|---|---|---|---|
| | | kann die Richtlinie nicht angewendet werden. | |
| Windows | BitLocker-Verschlüsselungsmethode für Mobilgeräte | Geben Sie die BitLocker Drive Encryption-Methode und die Verschlüsselungsstärke für Mobilgeräte an. Diese Regel gilt nicht für Windows 10-Computer und -Tablets. | MDM-Steuerelemente |
| Windows | BitLocker-Verschlüsselungsmethode für Desktop | Geben Sie die BitLocker Drive Encryption-Methode und die Verschlüsselungsstärke für Tablets und Computer an. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Eingabeaufforderungen zur Speicherkartenverschlüsselung auf dem Gerät zulassen | Legen Sie fest, ob das Gerät den Benutzer zur Verschlüsselung der Speicherkarte auffordert. Wenn diese Regel nicht ausgewählt ist, ist die Verschlüsselung nicht deaktiviert. Diese Regel gilt nicht für Windows 10-Computer und -Tablets. | MDM-Steuerelemente |
| Windows | BitLocker Device Encryption kann Verschlüsselung auf dem Gerät aktivieren | Legen Sie fest, ob BitLocker Device Encryption die Verschlüsselung auf dem Gerät aktivieren kann. Wenn diese Regel nicht ausgewählt ist, wird die Verschlüsselung nicht deaktiviert, aber der Benutzer wird nicht aufgefordert, sie zu aktivieren. | MDM-Steuerelemente |
| Windows | Standard-Verschlüsselungsmethoden für jeden Laufwerkstyp festlegen | Legen Sie fest, ob der von BitLocker Drive Encryption verwendete Standardalgorithmus | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| | | und die Verschlüsselungsstärke für verschiedene Laufwerkstypen separat konfiguriert werden können. Diese Regel gilt nicht für Windows 10-Smartphones. | |
| Windows | Verschlüsselungsmethode für Betriebssystemlaufwerke | Geben Sie die Verschlüsselungsmethode für Betriebssystemlaufwerke an. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Verschlüsselungsmethode für Festplattenlaufwerke | Geben Sie die Verschlüsselungsmethode für Festplattenlaufwerke an. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Verschlüsselungsmethode für Wechseldatenträger | Geben Sie die Verschlüsselungsmethode für Wechseldatenträger an. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Zusätzliche Authentifizierung beim Start erforderlich | Legen Sie fest, ob BitLocker bei jedem Start des Geräts eine zusätzliche Authentifizierung erfordert. Diese Einstellung wird angewendet, wenn BitLocker aktiviert ist. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | BitLocker ohne kompatiblen TPM zulassen | Legen Sie fest, ob BitLocker ohne TPM-Chip gestartet werden kann. Wenn diese Regel ausgewählt ist, kann BitLocker mit einem Kennwort oder einem Startschlüssel auf einem USB- | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| | | Flashlaufwerk gestartet werden. Diese Regel gilt nicht für Windows 10-Smartphones. | |
| Windows | TPM-Startschlüssel erforderlich | Geben Sie an, ob ein TPM-Startschlüssel optional, erforderlich oder nicht zulässig ist. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | TPM-Start-PIN erforderlich | Legen Sie fest, ob eine TPM-Start-PIN optional, erforderlich oder nicht zulässig ist. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | TPM-Startschlüssel und PIN erforderlich | Legen Sie fest, ob ein TPM-Startschlüssel und eine PIN optional, erforderlich oder nicht zulässig sind. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | TPM-Start erforderlich | Geben Sie an, ob der TPM-Start optional, erforderlich oder nicht zulässig ist. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Mindestlänge der PIN für den Start erforderlich | Geben Sie an, ob BitLocker eine PIN-Mindestlänge für den Start erfordert. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | PIN-Mindestlänge | Legen Sie die Mindestanzahl der PIN-Stellen für den Start fest. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| Windows | Pre-Boot-Wiederherstellungsmeldung und URL | Legen Sie fest, ob Sie die Meldung und URL für die Pre-Boot-Wiederherstellung von BitLocker anpassen können, die auf dem Bildschirm für die Pre-Boot-Schlüsselwiederherstellung angezeigt werden, wenn das Betriebssystemlaufwerk gesperrt ist. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Pre-Boot-Wiederherstellungsbildschirm | Geben Sie an, ob der BitLocker-Bildschirm für die Wiederherstellung vor dem Start leer ist, eine Standardmeldung und URL anzeigt, eine benutzerdefinierte Meldung anzeigt oder eine benutzerdefinierte URL anzeigt. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Benutzerdefinierte Wiederherstellungsmeldung | Wenn Sie „Benutzerdefinierte Wiederherstellungsmeldung“ in der Regel „Pre-Boot-Wiederherstellungsbildschirm“ ausgewählt haben, geben Sie die benutzerdefinierte Meldung an. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Benutzerdefinierte Wiederherstellungs-URL | Wenn Sie „Benutzerdefinierte Wiederherstellungs-URL“ in der Regel „Pre-Boot-Wiederherstellungsbildschirm“ ausgewählt haben, geben Sie die benutzerdefinierte URL | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| | | an. Diese Regel gilt nicht für Windows 10-Smartphones. | |
| Windows | BitLocker-Wiederherstellungsoptionen für Betriebssystemlaufwerke | Legen Sie fest, ob Sie anpassen können, wie mit BitLocker geschützte Betriebssystemlaufwerke wiederhergestellt werden, wenn die erforderlichen Startschlüsselinformationen fehlen. Diese Einstellung ist verfügbar, wenn Sie BitLocker aktivieren. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Zertifikatbasierten Datenwiederherstellungs-Agent für Betriebssystemlaufwerke zulassen | Legen Sie fest, ob ein Datenwiederherstellungs-Agent für durch BitLocker geschützte Betriebssystemlaufwerke verwendet werden kann. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Generierung des Wiederherstellungskennworts für Betriebssystemlaufwerke zulassen | Legen Sie fest, ob der Benutzer ein BitLocker-Wiederherstellungskennwort für Betriebssystemlaufwerke erstellen und speichern kann. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Generierung des Wiederherstellungsschlüssels für Betriebssystemlaufwerke zulassen | Legen Sie fest, ob der Benutzer einen BitLocker-Wiederherstellungsschlüssel für Betriebssystemlaufwerke erstellen und speichern kann. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Wiederherstellungsoptionen des BitLocker- | Legen Sie fest, ob Wiederherstellungsoptionen | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| | Einrichtungsassistenten für Betriebssystemlaufwerke ausschließen | für den Benutzer ausgeblendet werden, wenn BitLocker auf einem Betriebssystemlaufwerk aktiviert wird. | |
| Windows | Speichern von BitLocker-Wiederherstellungsinformationen für Betriebssystemlaufwerke auf Active Directory-Domänendiensten zulassen | Legen Sie fest, ob BitLocker-Wiederherstellungsinformationen für Betriebssystemlaufwerke in Active Directory-Domänendiensten gespeichert werden können. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Gespeicherte BitLocker-Wiederherstellungsinformationen für Betriebssystemlaufwerke | Legen Sie fest, ob Active Directory-Domänendienste nur Wiederherstellungskennwörter oder sowohl Wiederherstellungskennwörter als auch Schlüsselpakete für Betriebssystemlaufwerke speichern. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Sicherung von Active Directory für Wiederherstellungsinformationen für Betriebssystemlaufwerke erforderlich | Legen Sie fest, ob die in Active Directory-Domänendiensten gespeicherten BitLocker-Wiederherstellungsinformationen für Betriebssystemlaufwerke gesichert werden müssen. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | BitLocker-Wiederherstellungsoptionen für Festplattenlaufwerke | Legen Sie fest, ob Sie anpassen können, wie mit BitLocker geschützte Festplattenlaufwerke wiederhergestellt werden, wenn die | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| | | erforderlichen Startschlüsselinformationen fehlen. Diese Einstellung ist verfügbar, wenn Sie BitLocker aktivieren. Diese Regel gilt nicht für Windows 10-Smartphones. | |
| Windows | Zertifikatbasierten Datenwiederherstellungs-Agent für Festplattenlaufwerke zulassen | Legen Sie fest, ob ein Datenwiederherstellungs-Agent für durch BitLocker geschützte Festplattenlaufwerke verwendet werden kann. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Generierung von Wiederherstellungskennwörtern für Festplattenlaufwerke zulassen | Legen Sie fest, ob der Benutzer ein BitLocker-Wiederherstellungskennwort für Festplattenlaufwerke erstellen und speichern kann. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Generierung des Wiederherstellungsschlüssels für Festplattenlaufwerke zulassen | Legen Sie fest, ob der Benutzer einen BitLocker-Wiederherstellungsschlüssel für Festplattenlaufwerke erstellen und speichern kann. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Wiederherstellungsoptionen des BitLocker-Einrichtungsassistenten für Festplattenlaufwerke ausschließen | Legen Sie fest, ob Wiederherstellungsoptionen für den Benutzer ausgeblendet werden, wenn BitLocker auf einem Festplattenlaufwerke aktiviert wird. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Speichern von BitLocker-Wiederherstellungsinformationen | Speichern von BitLocker-Wiederherstellungsinformationen | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| | für Festplattenlaufwerke auf Active Directory-Domänendiensten zulassen | für Festplattenlaufwerke auf Active Directory-Domänendiensten zulassen. Diese Regel gilt nicht für Windows 10-Smartphones. | |
| Windows | Gespeicherte BitLocker-Wiederherstellungsinformationen für Festplattenlaufwerke | Legen Sie fest, ob Active Directory-Domänendienste nur Wiederherstellungskennwörter oder sowohl Wiederherstellungskennwörter als auch Schlüsselpakete für Festplattenlaufwerke speichern. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Sicherung von Active Directory für Wiederherstellungsinformationen für Festplattenlaufwerke erforderlich | Legen Sie fest, ob die in Active Directory-Domänendiensten gespeicherten BitLocker-Wiederherstellungsinformationen für Festplattenlaufwerke gesichert werden müssen. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | BitLocker-Schutz für Festplatten-Datenlaufwerke erforderlich | Legen Sie fest, ob der BitLocker-Schutz erforderlich ist, um Schreibzugriff auf Festplatten-Datenlaufwerke zu ermöglichen. Wenn diese Regel ausgewählt ist, werden alle nicht mit BitLocker geschützten Festplatten-Datenlaufwerke schreibgeschützt geladen. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| Windows | BitLocker-Schutz für Wechseldatenträger erforderlich | Legen Sie fest, ob der BitLocker-Schutz erforderlich ist, um Schreibzugriff auf Wechseldatenträger-Laufwerke zu ermöglichen. Wenn diese Regel ausgewählt ist, werden alle Wechseldatenträger-Laufwerke, die nicht mit BitLocker geschützt sind, schreibgeschützt gemountet. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Schreibzugriff auf Geräte mit Konfiguration einer anderen Organisation zulassen | Legen Sie fest, ob Wechseldatenträger, die nicht mit den ID-Feldern des Geräts übereinstimmen, Schreibzugriff erhalten können. Wenn diese Regel ausgewählt ist, erhalten nur Laufwerke mit Identifikationsfeldern Schreibzugriff, die den Identifikationsfeldern des Computers entsprechen. Diese Regel gilt nicht für Windows 10-Smartphones. | MDM-Steuerelemente |
| Windows | Eingabeaufforderung für Speicherort des Wiederherstellungsschlüssels zulassen | Legen Sie fest, ob der Benutzer über eine Eingabeaufforderung auswählen kann, wo der Wiederherstellungsschlüssel des Betriebssystemlaufwerks gesichert werden soll. Wenn diese Regel nicht ausgewählt ist, wird der Wiederherstellungsschlüssel des Betriebssystemlaufwerks im Azure Active Directory-Konto des Benutzers gesichert. | MDM-Steuerelemente |

| | | | |
|---|---|---|---|
| | | Diese Regel gilt nicht für Windows 10-Smartphones. | |
| Windows | Verschlüsselung für Standardbenutzer aktivieren | Legen Sie fest, ob die Verschlüsselung auf allen Festplattenlaufwerken aktiviert ist, auch wenn es sich bei dem aktuell angemeldeten Benutzer um einen Standardbenutzer handelt. Diese Einstellung wird nur auf Windows 10-Smartphones mit Azure Active Directory unterstützt. | MDM-Steuerelemente |

# Was ist BlackBerry UEM ?

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

Sie können BlackBerry UEM in einer lokalen Umgebung installieren, um die größtmögliche Kontrolle über Ihre Server, Daten und Geräte zu erhalten, oder Sie können BlackBerry UEM Cloud verwenden, was eine benutzerfreundliche, kostengünstige und sichere Lösung bietet. BlackBerry hostet BlackBerry UEM Cloud über das Internet. Sie benötigen lediglich einen unterstützten Webbrowser, um auf diesen Dienst zuzugreifen.

Sowohl BlackBerry UEM lokal als auch BlackBerry UEM Cloud bieten vertrauenswürdige durchgehende Sicherheit und die für Unternehmen erforderliche Kontrolle, um alle Endpunkte und Eigentümermodelle zu verwalten.

Zu den Vorteilen von BlackBerry UEM zählen unter anderem:

| Funktion | Vorteil |
|---|---|
| Geringe Gesamtbetriebskosten | BlackBerry UEM (lokal) reduziert die Komplexität, optimiert die Poolressourcen, sorgt für eine maximale Betriebszeit und unterstützt Sie bei der Erzielung der geringstmöglichen Gesamtbetriebskosten für eine lokale Lösung.<br>BlackBerry UEM Cloud senkt die Betriebskosten, da keine Services installiert, verwaltet und aktualisiert werden müssen. |
| Eine einzige webbasierte Schnittstelle | Verwaltung von iOS-, macOS-, Android-, Windows 10- und BlackBerry 10-Geräten und weiteren BlackBerry Secure UEM & Productivity Suite-Diensten über eine einzige Verwaltungskonsole. |
| Flexible Eigentümermodelle | Verwendung einer Reihe von anpassbaren Richtlinien und Profilen zur Verwaltung von BYOD-, COPE- und COBO-Geräten sowie zum Schutz von Geschäftsinformationen. |
| Berichtserstellung zu Benutzern und Geräten | Verwaltung von Gerätebeständen über ein umfassendes Berichtswesen und Dashboards, dynamische Filter und robuste Suchfunktionen |
| Problemlose Einrichtung und Registrierung von Benutzern | Aktivierung benutzereigener Geräte mit BlackBerry UEM Self-Service. |
| Branchenführende Sicherheit für mobile Geräte | Einsatz von BlackBerry Infrastructure, um für Datensicherheit auf allen Geräten zu sorgen. |
| Hohe Verfügbarkeit | Konfigurieren Sie hohe Verfügbarkeit für lokale Umgebungen, um Serviceunterbrechungen für Gerätebenutzer zu minimieren, oder verlassen Sie sich bei der Wartung von BlackBerry UEM Cloud und der Maximierung der Laufzeit auf BlackBerry. |
| Weitere Dienste verfügbar | Aktivieren Sie Dienste wie BlackBerry Workspaces, BlackBerry Enterprise Identity, BlackBerry 2FA, BBM Enterprise und BlackBerry UEM Notifications, mit denen Sie den Wert Ihrer BlackBerry UEM-Bereitstellung steigern können. |

Weitere Informationen zu BlackBerry UEM finden Sie in der Dokumentation für Administratoren.

# BlackBerry-Enterprise-Dienste

Neben den von BlackBerry UEM gebotenen Sicherheits- und Produktivitätsfunktionen bietet BlackBerry weitere Dienste, mit denen Sie den Wert von BlackBerry UEM steigern und die individuellen Anforderungen Ihres Unternehmens erfüllen können. Sie können die nachfolgenden Dienste hinzufügen und sie über die BlackBerry UEM-Verwaltungskonsole verwalten:

| Diensttyp | Name und Beschreibung des Dienstes |
|---|---|
| Enterprise-Dienste | • BlackBerry Workspaces ermöglicht Benutzern das sichere Zugreifen auf, Synchronisieren, Bearbeiten und Freigeben von Dateien und Ordnern auf Windows- und Mac OS-Tablets und -Computern sowie auf Android-, iOS und BlackBerry 10-Geräten. BlackBerry Workspaces schützt Dateien durch die Anwendung von DRM-Steuerelementen, um den Zugriff auch bei gemeinsamer Verwendung außerhalb Ihres Unternehmens einzuschränken.<br>• BlackBerry Enterprise Identity ermöglicht den Zugriff per einmaliger Anmeldung (Single Sign-On, SSO) auf Dienstanbieter wie BlackBerry Workspaces, Box, Workday, WebEx, Salesforce und viele weitere. Sie können auch Unterstützung für benutzerdefinierte SaaS-Dienste hinzufügen.<br>• BlackBerry 2FA schützt den Zugriff auf die kritischen Ressourcen Ihres Unternehmens mithilfe der Zwei-Faktor-Authentifizierung. BlackBerry 2FA fordert ein Kennwort von Benutzern und zeigt jedes Mal eine Sicherheitsaufforderung auf ihrem Android-, iOS- oder BlackBerry 10-Gerät an, wenn diese auf Ressourcen zugreifen möchten. |
| BlackBerry Dynamics-Plattform | • Der BlackBerry Enterprise Mobility Server (BEMS) lokal und BEMS-Cloud bietet zusätzliche Dienste für BlackBerry Dynamics-Apps.<br>  • BEMS lokal integriert BlackBerry Mail, BlackBerry Connect, BlackBerry Presence und BlackBerry Docs-Dienste. Wenn diese Dienste integriert wurden, können Benutzer über sichere E-Mail-Nachrichten und Instant Messaging miteinander kommunizieren, die Verfügbarkeit von Benutzern in BlackBerry Dynamics-Apps in Echtzeit abrufen und auf geschäftliche Dateiserver, Microsoft SharePoint-, Microsoft SharePoint Online-, Microsoft OneDrive for Business- und Box-Dokumente zugreifen, diese synchronisieren und teilen.<br>  • BEMS lokal integriert BlackBerry Mail- und BlackBerry Docs-Dienste. Wenn diese Dienste integriert sind, können Benutzer über sichere E-Mail-Nachrichten miteinander kommunizieren und auf Microsoft SharePoint-, Microsoft SharePoint Online-, Microsoft OneDrive for Business- und Box-Dokumente zugreifen, diese synchronisieren, und freigeben, ohne dass dabei geschäftliche Daten gefährdet werden.<br>• Das BlackBerry Dynamics SDK ermöglicht es den Entwicklern, sichere Apps für Android- und iOS-Geräte sowie Mac OS- und Windows-Computer zu erstellen. |

| Diensttyp | Name und Beschreibung des Dienstes |
| --- | --- |
| BlackBerry Dynamics-Produktivitätsanwendungen | • BlackBerry Work beinhaltet alles, was Benutzer benötigen, um sicher mobil zu arbeiten, darunter Zugriff auf E-Mails, Kalender und Kontakte (vollständige Synchronisierung mit Microsoft Exchange). Die App ermöglicht zudem erweiterte Zusammenarbeitsfunktionen für Dokumente. BlackBerry Work trennt geschäftliche von persönlichen Daten und kann problemlos auch ohne MDM-Profile auf dem Gerät in andere geschäftliche Apps integriert werden.<br>• BlackBerry Access ermöglicht den Benutzern, von ihrem Gerät aus über eine sichere Verbindung auf das Intranet des Unternehmens zuzugreifen.<br>• BlackBerry Connect verbessert die Kommunikation und Zusammenarbeit mit sicherem Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen über eine benutzerfreundliche Schnittstelle auf dem Gerät des Benutzers.<br>• BlackBerry Tasks ermöglicht Benutzern, Notizen, die mit Microsoft Exchange auf Android- und iOS-Geräten synchronisiert wurden, zu erstellen, zu bearbeiten und zu verwalten.<br>• BlackBerry Notes ermöglicht es Benutzern, Notizen, die sie auf ihrem Gerät mit Microsoft Exchange synchronisiert haben, zu erstellen, zu bearbeiten und zu verwalten. |

Diese Services können als Teil einer BlackBerry Secure UEM & Productivity Suite-Lizenz erworben werden. Weitere Informationen zu den unterschiedlichen BlackBerry Secure UEM & Productivity Suite-Lizenzen und zu ihrem Erwerb finden Sie in der Dokumentation zur Lizenzierung.

# BlackBerry Secure UEM & Productivity Suites

BlackBerry Secure UEM & Productivity Suites umfassen BlackBerry UEM, BlackBerry Dynamics und weitere Dienste unter einer einzigen Lizenz und bieten so eine umfassende einheitliche Endpunktverwaltungslösung, welche mobile Zusammenarbeit und einen vertrauenswürdigen durchgehenden Sicherheitsansatz bereitstellt.

| Suite | Funktionen |
| --- | --- |
| BlackBerry Secure UEM & Productivity Suites – Choice Suite | • Plattformübergreifende Unterstützung für iOS-, macOS-, Android- (einschließlich Samsung Knox), Windows 10- und BlackBerry 10-Geräte<br>• BlackBerry UEM mit Unterstützung von Geschäftlich und persönlich – Unternehmen-Aktivierungen für BlackBerry 10-Geräte, MDM-Steuerelemente für die meisten Gerätetypen, Benutzerdatenschutzaktivierungen für iOS- und Android-Geräte sowie geschäftlichen, persönlichen und Nur geschäftlicher Bereich-Aktivierungen für Android-Geräte<br>• BlackBerry Dynamics mit Unterstützung für MDM, MAM, BlackBerry Access und BlackBerry Work<br>• Sicheres Instant Messaging mit BlackBerry Connect<br>• Bereitstellungsoptionen für die Cloud und vor Ort<br>• Sammeln der Daten und Nutzungskennzahlen von BlackBerry Dynamics-Apps auf den Geräten der Benutzer mithilfe von BlackBerry Analytics. |

| Suite | Funktionen |
| --- | --- |
| BlackBerry Secure UEM & Productivity Suites – Freedom Suite | • Alle BlackBerry Secure UEM & Productivity Suites – Choice Suite-Funktionen<br>• Erweiterte BlackBerry UEM-Sicherheits- und Konnektivitätsfunktionen für die Verwaltung von iOS-, Android- (einschließlich Samsung Knox Workspace und Knox Platform for Enterprise) und BlackBerry 10-Geräten<br>• Sicherer Zugriff auf Arbeitsinhalte mit BlackBerry Secure Connect Plus und BlackBerry Docs<br>• Unbeschränkte Bereitstellung mit BlackBerry Dynamics gesicherten Apps von externen Softwareherstellern<br>• Sicherer Zugriff zum Anzeigen, Bearbeiten und Speichern von Dokumenten mit von Intune verwalteten Microsoft -Apps, wie Microsoft Word, Microsoft PowerPoint und Microsoft Excel, in BlackBerry Dynamics-Apps auf iOS- und Android-Geräten mit BlackBerry Enterprise BRIDGE<br>• Vollständiger Cloud-Serviceverbund und Single-Sign-On-Lösung mit BlackBerry Enterprise Identity<br>• Unbeschränkte Bereitstellung von kundeneigenen gesicherten BlackBerry Dynamics-Apps<br>• App-Integration von benutzerdefinierten gemeinsamen Diensten<br>• Mit BlackBerry 2FA durch die Geräte von Benutzern aktivierte Zwei-Faktor-Authentifizierung<br>• Dateisynchronisierung, Freigabe und Zugriffssteuerung für Unternehmen mit BlackBerry Workspaces |
| BlackBerry Secure UEM & Productivity Suites – Limitless Suite | • Alle BlackBerry Secure UEM & Productivity Suites – Freedom Suite-Funktionen<br>• Direkt über die BlackBerry UEM-Verwaltungskonsole mit UEM Notifications Mitteilungen per SMS, Telefon und E-Mail an Benutzer zu senden<br>• Dateisynchronisierung, Freigabe, Zugriffskontrolle, Verwaltung von Dokumentrechten auf Mobilgeräten und SDK-Unterstützung für Unternehmen mit BlackBerry Workspaces |

# Vorteile von BlackBerry Workspaces

BlackBerry Workspaces ist eine Dateiverwaltungsplattform für Unternehmen, über die Benutzer sicher auf Dateien und Ordner auf verschiedenen Geräten zugreifen und diese synchronisieren, bearbeiten und freigeben können. BlackBerry Workspaces mindert das Risiko von Datenverlust oder Diebstahl durch die Einbettung eines integrierten Schutzes zur Verwaltung von digitalen Rechten in jeder Datei, sodass Ihre Inhalte weiterhin sicher sind und unter Ihrer Kontrolle bleiben, auch nachdem sie heruntergeladen und für andere freigegeben wurden. Durch sicheres Speichern von Dateien und die Möglichkeit, Daten zu übertragen und dabei die Kontrolle zu behalten, können Mitarbeiter und die IT-Abteilung problemlos Daten freigeben und sich auf Dokumentensicherheit verlassen.

Benutzer können auf BlackBerry Workspaces über einen Webbrowser und Apps auf Windows- und macOS-Computern sowie auf iOS-, Android- und BlackBerry 10-Geräten zugreifen. Inhalte werden auf allen Geräten eines Benutzers synchronisiert, wenn er online ist, sodass er Dateien von jedem Gerät aus verwalten, anzeigen, erstellen, bearbeiten und kommentieren kann. Außerdem können Sie das Workspaces-Plug-In für BlackBerry UEM verwenden, um die Workspaces-Verwaltung in die BlackBerry UEM-Verwaltungskonsole zu integrieren.

Falls Ihr Unternehmen auch BlackBerry Enterprise Identity implementiert hat, können Sie Enterprise Identity zur Verwaltung der Benutzerberechtigung für Workspaces verwenden. Weitere Informationen zu Enterprise Identity finden Sie in der BlackBerry Enterprise Identity-Dokumentation.

BlackBerry Workspaces kann separat oder zusammen mit der BlackBerry Secure UEM & Productivity Suites – Freedom Suite erworben oder lizenziert werden. Weitere Funktionen sind in BlackBerry Secure UEM & Productivity Suites – Limitless Suite enthalten.

Weitere Informationen finden Sie in der Dokumentation zu BlackBerry Workspaces.

# Vorteile von BlackBerry Enterprise Identity

BlackBerry Enterprise Identity erleichtert Benutzern den Zugriff auf Cloud-Anwendungen von jedem Gerät aus, z. B. von iOS, Android und BlackBerry 10 sowie von herkömmlichen Rechenplattformen. Diese Funktion ist eng mit BlackBerry UEM verflochten und vereint so eine branchenführende EMM-Lösung mit dem Anspruch auf Nutzung und der Möglichkeit der Kontrolle für all Ihre Cloud-Dienste.

BlackBerry Enterprise Identity bietet Single Sign-On (SSO) für Cloud-Dienste, wie z. B. Microsoft Office 365, G Suite, BlackBerry Workspaces und viele andere. Bei der einmaligen Anmeldung (Single Sign-On) müssen Benutzer nicht mehrere Anmeldungen ausführen oder sich mehrere Kennwörter merken. Administratoren können außerdem benutzerdefinierte Dienste zu Enterprise Identity hinzufügen, um Benutzern Zugriff auf interne Anwendungen zu ermöglichen.

Administratoren können mit der BlackBerry UEM-Verwaltungskonsole Dienste hinzufügen, Benutzer verwalten und weitere Administratoren hinzufügen und verwalten. Die Integration in BlackBerry UEM vereinfacht die Verwaltung von Benutzern und gewährt ihnen Zugriff auf Cloud-Anwendungen und -Dienste über ihre Geräte. Mit BlackBerry UEM können Cloud-Dienste und die Binärdateien mobiler Apps gebündelt und dann auf einfache Weise einem Benutzer oder einer Gruppe von Benutzern zugewiesen werden.

Enterprise Identity kann separat oder zusammen mit den BlackBerry Secure UEM & Productivity Suites erworben oder lizenziert werden.

- Choice Suite
- Freedom Suite
- Limitless Suite

Weitere Informationen zu Enterprise Identity finden Sie in der Dokumentation zu BlackBerry Enterprise Identity.

# Vorteile von BlackBerry 2FA

BlackBerry 2FA ermöglicht Benutzern die Verwendung der Zwei-Faktor-Authentifizierung für den Zugriff auf Unternehmensressourcen. Benutzer können ihre iOS-, Android- und BlackBerry 10-Geräte als zweiten Faktor für die Authentifizierung verwenden, wenn sie eine Verbindung zu den Ressourcen Ihres Unternehmens herstellen. BlackBerry 2FA interagiert auf einfache Weise mit den Benutzern, indem es sie zur Eingabe einer Bestätigung auf ihrem Gerät auffordert, wenn sie versuchen, auf Ressourcen zuzugreifen.

Für Benutzer, die nicht über ein mobiles Gerät verfügen oder deren Mobilgerät keine ausreichende Verbindung für die Unterstützung von Echtzeit-BlackBerry 2FA aufweisen, können standardbasierte Einmalkennwort-Token (OTP, One-Time Password) ausgegeben werden. Die erste Authentifizierungsstufe bildet das Verzeichniskennwort des Benutzers und die zweite Authentifizierungsstufe ein dynamischer Code, der auf dem Token-Bildschirm angezeigt wird.

Sie verwalten BlackBerry 2FA von der BlackBerry UEM- oder BlackBerry UEM Cloud-Verwaltungskonsole aus. BlackBerry 2FA ist auch in BlackBerry Enterprise Identity integriert. Sie können mit BlackBerry 2FA einen zweiten Faktor der Authentifizierung für diejenigen Ressourcen bereitstellen, deren Zugriff Sie mit Enterprise Identity verwalten.

BlackBerry 2FA kann separat oder zusammen mit den BlackBerry Secure UEM & Productivity Suites erworben oder lizenziert werden.

- Freedom Suite
- Limitless Suite

Weitere Informationen zu BlackBerry 2FA finden Sie in der Dokumentation zu BlackBerry 2FA.

# Vorteile von BlackBerry UEM Notifications

BlackBerry UEM Notifications nutzt das BlackBerry AtHoc Networked Crisis Communication-System, um Administratoren das Versenden wichtiger Nachrichten und Benachrichtigungen an Benutzer und Gruppen von der UEM-Managementkonsole aus zu ermöglichen.

Da UEM Notifications es Administratoren erlaubt, Geräte und Benachrichtigungen in der UEM-Verwaltungskonsole zu verwalten, müssen sie Kontaktinformationen der Benutzer nicht auf mehreren Systemen verwalten und abgleichen und sich nicht mit Zugriffsproblemen in externen Systemen befassen. UEM Notifications verwendet Kontaktinformationen mithilfe der Microsoft Active Directory-Synchronisation. UEM Notifications bietet zudem flexible Bereitstellungsoptionen, beispielsweise Text-To-Speech-Sprachanrufe, SMS und E-Mail, sodass Benutzer Warnmeldungen über ihren bevorzugten Kanal erhalten und schneller reagieren können.

Administratoren können gesendete Benachrichtigungen verfolgen und verwalten, darunter einen detaillierten Nachrichtenstatus nach Bereitstellungsmethode. UEM Notifications verwendet von FedRAMP autorisierte Bereitstellungsdienste und stellt einen umfassenden Bericht über alle gesendeten Nachrichten und deren Status zur Verfügung.

BlackBerry UEM Notifications kann separat mit BlackBerry UEM oder zusammen mit BlackBerry Secure UEM & Productivity Suites – Limitless Suite erworben oder lizenziert werden.

Weitere Informationen zu UEM Notifications finden Sie in der Dokumentation zu UEM Notifications.

# Apps für Unternehmen

BlackBerry bietet unterschiedliche Apps für Unternehmen, die Administratoren per Push auf Geräte übertragen oder von Benutzern für einen einfacheren Zugriff auf geschäftliche Daten und höhere Produktivität installiert werden können.

| Komponente | Beschreibung |
| --- | --- |
| BlackBerry UEM Client | Das BlackBerry UEM Client gestattet BlackBerry UEM die Verwaltung von iOS- und Android-Geräten. Benutzer benötigen BlackBerry UEM Client, wenn sie iOS- oder Android-Geräte für die Verwaltung mobiler Geräte mit BlackBerry UEM aktivieren möchten. Benutzer können die aktuelle Version des BlackBerry UEM Client für iOS-Geräte von App Store und für Android-Geräte von Google Play herunterladen. Nachdem Benutzer ihre Geräte aktiviert haben, bietet der BlackBerry UEM Client folgende Möglichkeiten:<br>• Überprüfung der Kompatibilität ihrer Geräte mit den Standards des Unternehmens<br>• Ansicht der Profile, die ihren Benutzerkonten zugewiesen sind<br>• Ansicht der IT-Richtlinienregeln, die ihren Benutzerkonten zugewiesen sind<br>• Zugriff auf geschäftliche Apps<br>• Erstellen von Zugriffsschlüsseln für BlackBerry Dynamics-Apps<br>• Vorauthentifizierung mit BlackBerry 2FA<br>• Zugriff auf einen Software-OTP-Code<br>• Abrufen und Versenden von Geräteprotokolldateien per E-Mail<br>• Deaktivieren ihrer Geräte<br>Weitere Informationen finden Sie in der Dokumentation zu BlackBerry UEM Client. |
| BlackBerry Dynamics-Apps | BlackBerry Dynamics-Produktivitäts-Apps wie z. B. BlackBerry Work, BlackBerry Access und BlackBerry Connect ermöglichen Benutzern den Zugriff auf geschäftliche Daten und Produktivitäts-Tools. Weitere Informationen finden Sie in der Dokumentation zu der jeweiligen App. |
| BBM Enterprise | BBM Enterprise fügt eine zusätzliche Schicht für die durchgehende Verschlüsselung von BBM-Nachrichten hinzu, die zwischen BBM Enterprise-Benutzern in Ihrem Unternehmen und anderen BBM-Benutzern innerhalb und außerhalb Ihres Unternehmens ausgetauscht werden. BBM Enterprise ist für iOS-, Android-, BlackBerry 10-, Windows- und macOS-Geräte verfügbar.<br>BBM Enterprise verwendet eine nach FIPS 140-2 validierte kryptographische Bibliothek. Die Verschlüsselungsschlüssel gehören Ihrem Unternehmen und sonst niemandem. Nicht einmal BlackBerry kann darauf zugreifen.<br>Bei den meisten Geräten können Sie Benutzern mithilfe von BlackBerry UEM BBM Enterprise zuweisen. Nach der Aktivierung der Benutzer für die Verwendung von BBM Enterprise können Benutzer die BBM Enterprise-App beim App Store, beim Google Play oder bei BlackBerry World herunterladen. Weitere Informationen zu BBM Enterprise finden Sie in der Dokumentation zu BBM Enterprise. |
| BlackBerry Enterprise BRIDGE | BlackBerry Enterprise BRIDGE ist eine für BlackBerry Dynamics aktivierte Microsoft Intune-App. Sie ermöglicht Ihnen die sichere Anzeige, Bearbeitung und Speicherung von Dokumenten mithilfe von Intune-verwalteten Microsoft-Apps, wie Microsoft Word, Microsoft PowerPoint und Microsoft Excel in BlackBerry Dynamics auf iOS- und Android-Geräten.<br>Weitere Informationen zu BlackBerry Enterprise BRIDGE finden Sie in der Dokumentation zu BlackBerry Enterprise BRIDGE. |

## BlackBerry Dynamics-Apps

Die Produktivitäts-Apps von BlackBerry Dynamics ermöglichen Benutzern den Zugriff auf geschäftliche Daten und Produktivitäts-Tools. Zu den von BlackBerry entwickelten BlackBerry Dynamics-Apps gehören beispielsweise:

| App | Beschreibung |
| --- | --- |
| BlackBerry Work | Die BlackBerry Work-App bietet sicheren Zugriff auf geschäftliche E-Mails und ermöglicht Benutzern das Anzeigen und Senden von Anlagen, Erstellen benutzerdefinierter Benachrichtigungen und das Verwalten ihrer Nachrichten.<br>Weitere Informationen zu BlackBerry Work finden Sie in der Dokumentation zu BlackBerry Work. |
| BlackBerry Access | BlackBerry Access ist ein sicherer Browser, der Benutzern den Zugriff auf das geschäftliche Intranet und Webanwendungen ermöglicht. BlackBerry Access ermöglicht Ihnen zudem den Zugang zu Ressourcen an Ihrem Arbeitsplatz oder das Erstellen und Bereitstellen von HTML5-Apps, während gleichzeitig ein hohes Maß an Sicherheit und Richtlinientreue gewährleistet wird.<br>Weitere Informationen zu BlackBerry Access finden Sie in der Dokumentation zu BlackBerry Access. |
| BlackBerry Connect | BlackBerry Connect unterstützt Kommunikation und Zusammenarbeit mit sicherem Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen über eine benutzerfreundliche Schnittstelle auf dem Gerät des Benutzers.<br>Weitere Informationen zu BlackBerry Connect finden Sie in der Dokumentation zu BlackBerry Connect. |
| BlackBerry Tasks | BlackBerry Tasks ermöglicht Benutzern das Erstellen, Bearbeiten und Verwalten von Aufgaben und deren Synchronisierung mit Microsoft Exchange.<br>Weitere Informationen zu BlackBerry Tasks finden Sie in der Dokumentation zu BlackBerry Tasks. |
| BlackBerry Notes | BlackBerry Notes ermöglicht es Benutzern, Notizen, die mit Microsoft Exchange auf einem beliebigen Mobilgerät synchronisiert wurden, zu erstellen, zu bearbeiten und zu verwalten.<br>Weitere Informationen zu BlackBerry Notes finden Sie in der Dokumentation zu BlackBerry Notes. |

Darüber hinaus haben Sie die Möglichkeit, BlackBerry Dynamics-Apps zu verwenden, die von einem der externen Anwendungspartner von BlackBerry entwickelt wurden. Eine vollständige Liste der verfügbaren Apps finden Sie unter BlackBerry Marketplace for Enterprise Software.

Sie können auch mithilfe des BlackBerry Dynamics-SDK eigene BlackBerry Dynamics-Apps entwickeln. Weitere Informationen finden Sie in der Dokumentation für BlackBerry Dynamics-SDK.

# Unternehmens-SDKs

BlackBerry bietet mehrere Optionen für SDK, mit denen Ihr Unternehmen Ihre BlackBerry-Lösung anpassen und erweitern kann.

| Komponente | Beschreibung |
| --- | --- |
| BlackBerry UEM Integration SDK | Der BlackBerry UEM Integration SDK ermöglicht Entwicklern die Erstellung von Plug-ins, die die Funktionalität von BlackBerry UEM erweitern. Mithilfe von UEM Integration SDK (einschließlich UEM-Integrations-Plug-in für Eclipse) und den UEM-Integrations-APIs, können Sie die BlackBerry UEM-Plug-ins erzeugen und bereitstellen, mit denen eine enge Integration von neuen Funktionen oder Services in eine bestehende BlackBerry UEM-Installation möglich ist.<br><br>Weitere Informationen zu BlackBerry UEM Integration SDK finden Sie in der Dokumentation BlackBerry UEM Integration SDK. |
| BlackBerry Dynamics SDK | Das BlackBerry Dynamics SDK bietet eine leistungsstarke Reihe von Tools für ISV- und Unternehmensentwickler, damit sie sich auf die Entwicklung ihrer Apps konzentrieren können, anstatt zu lernen, wie sie diese Apps sichern, bereitstellen und verwalten. Das BlackBerry Dynamics SDK kann zur Entwicklung von nativen, hybriden und Web-Apps für iOS-, macOS-, Android- und Windows-Geräte mit Services wie den Folgenden verwendet werden:<br><br>• Sicherheitsdienste (z. B. sichere Kommunikation und APIs für den Datenaustausch zwischen Apps)<br>• Mobile Dienste (z. B. Anwesenheit, E-Mail, Push, Directory Lookup)<br>• Plattformservices (z. B. Authentifizierung per einmaliger Anmeldung, Identitäts- und Zugriffsmanagement, App-Steuerelemente für Administratoren)<br><br>Weitere Informationen zu BlackBerry Dynamics SDK finden Sie in der Dokumentation BlackBerry Dynamics SDK. |
| BlackBerry Analytics SDK | Mit dem BlackBerry Analytics SDK können Entwickler von BlackBerry Dynamics-Apps benutzerdefinierte BlackBerry Dynamics-Apps für Android und iOS aktivieren, um Ereignisse automatisch aufzuzeichnen und an BlackBerry Analytics zu senden. Sie müssen nur die BlackBerry Analytics-Bibliothek in Ihre App integrieren. Das SDK versendet die Veranstaltungen für Sie.<br><br>Weitere Informationen zu BlackBerry Analytics SDK finden Sie in der Dokumentation BlackBerry Analytics. |

| Komponente | Beschreibung |
| --- | --- |
| Spark Communications Services-SDK | Das BlackBerry Spark Communications Services-SDK bietet einen Rahmen für die Entwicklung von sicheren Echtzeit-, End-to-End-Messaging-Funktionen in Ihrem eigenen Produkt oder Service. Das Spark Communications Services-Sicherheitsmodell gewährleistet, dass nur der Sender und der beabsichtigte Empfänger die gesendete Nachricht anzeigen können, und dass Nachrichten während der Übertragung vom Absender zum Empfänger nicht geändert werden.<br><br>Das Spark Communications Services-SDK stellt außerdem den Rahmen für andere Formen der Zusammenarbeit und Kommunikation bereit, wie Push-Benachrichtigungen, sichere Sprach- und Videoanrufe und Dateifreigabe. Sie können sogar noch weiter gehen und neue Arten von Echtzeit-Services und Anwendungsfällen erstellen, indem Sie Ihre eigenen benutzerdefinierten Anwendungsprotokolle und Datentypen definieren.<br><br>Weitere Informationen zum Spark Communications Services finden Sie in der Dokumentation zum Spark Communications Services-SDK. |
| BlackBerry Web Services | Bei den BlackBerry Web Services handelt es sich um eine Sammlung von SOAP- und REST-Webdiensten, mit denen Sie Anwendungen zur Verwaltung der BlackBerry UEM-Domäne, der Benutzerkonten und aller unterstützten Geräte Ihres Unternehmens erstellen können. Sie können die BlackBerry Web Services zum Automatisieren zahlreicher Aufgaben verwenden, die von Administratoren üblicherweise über die Verwaltungskonsole durchgeführt werden. Sie können beispielsweise eine Anwendung erstellen, die das Erstellen von Benutzerkonten, das Hinzufügen von Benutzern zu mehreren Gruppen und das Verwalten von Benutzergeräten automatisiert.<br><br>Weitere Informationen zu BlackBerry Web Services finden Sie in der Dokumentation zu BlackBerry Web Services für BlackBerry UEM. |

Weitere Informationen zu Erwerb und Verwendung aller von BlackBerry verfügbaren Entwicklertools finden Sie auf der BlackBerry-Entwicklerseite.

# Wichtigste Funktionen von BlackBerry UEM

| Funktion | Beschreibung |
| --- | --- |
| Plattformübergreifende Geräteverwaltung | Sie können Geräte mit iOS, macOS, Android, Windows 10 und BlackBerry 10 verwalten. |
| Einheitliche, intuitiv bedienbare Benutzeroberfläche | Sie können alle Geräte an einem Ort anzeigen und alle Verwaltungsaufgaben über eine einzelne webbasierte Benutzerschnittstelle aufrufen. Sie können Verwaltungsaufgaben für mehrere Administratoren freigeben, die gleichzeitig auf die Verwaltungskonsole zugreifen können. Sie können zwischen Standard- und erweiterten Ansichten umschalten, um Optionen für die Anzeige von Informationen und das Filtern der Benutzerliste zu sehen. |
| Zuverlässige und sichere Benutzererfahrung | Steuerungsfunktionen für Geräte ermöglichen eine präzise Verwaltung der Verbindung von Geräten mit dem Netzwerk, der aktivierten Funktionen und der verfügbaren Apps. Die Unternehmensdaten werden geschützt, ungeachtet dessen, ob die Geräte sich im Besitz Ihres Unternehmens oder Ihrer Benutzer befinden. |
| Trennung geschäftlicher und persönlicher Anforderungen | Sie können Geräte mit den Technologien Android Enterprise, Samsung Knox und BlackBerry Balance verwalten. Diese zielen darauf ab, persönliche und geschäftliche Informationen auf den Geräten zu trennen und sichern. Wenn ein Gerät verloren geht oder der Mitarbeiter das Unternehmen verlässt, können Sie nur die geschäftlichen oder alle Daten vom Gerät löschen. |
| Sichere IP-Konnektivität | Mit BlackBerry Secure Connect Plus können Sie einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf BlackBerry 10-, iOS-, Samsung Knox Workspace- und Android-Geräten mit Arbeitsprofil und dem Netzwerk des Unternehmens bereitstellen. Über diesen Tunnel haben Benutzer Zugriff auf Ressourcen hinter der Firewall des Unternehmens, wobei die Sicherheit der Daten mithilfe standardmäßiger IPv4-Protokolle (TCP und UDP) und durchgehender Verschlüsselung sichergestellt wird. |
| Einfacher Self-Service für Benutzer | BlackBerry UEM Self-Service senkt die Zahl der Support-Anfragen und die IT-Kosten und ermöglicht gleichzeitig eine Durchführung gerätebezogener Arbeiten innerhalb eines angemessenen Zeitrahmens. Benutzer können mit BlackBerry UEM Self-Service verschiedene Aufgaben erledigen, z. B. Geräte aktivieren oder wechseln, das Gerätekennwort per Fernzugriff ändern, Gerätedaten löschen, ein Gerät nach Verlust oder Diebstahl sperren und andere wichtige Support-Anforderungen erfüllen. |

| Funktion | Beschreibung |
| --- | --- |
| Integration in Dienste wie beispielsweise BlackBerry Workspaces, BlackBerry Enterprise Identity und BlackBerry 2FA | Sie können BlackBerry UEM in BlackBerry Workspaces, BlackBerry Enterprise Identity und BlackBerry 2FA integrieren, mit denen Sie den Wert der BlackBerry UEM-Instanz Ihres Unternehmens steigern können. |
| Leistungsstarke App-Verwaltung | BlackBerry UEM ist eine umfassende App-Verwaltungsplattform für alle Geräte. Sie können Apps aus allen wichtigen App Stores, einschließlich App Store, Google Play, Windows Store und BlackBerry World-Storefront, bereitstellen. |
| Rollenbasierte Verwaltung | Sie können Verwaltungsaufgaben für andere Administratoren freigeben, die gleichzeitig auf die Administrationskonsolen zugreifen können. Sie können mithilfe von Rollen die Aktionen definieren, die ein Administrator ausführen kann, und durch die Beschränkung der Optionen für die einzelnen Administratoren Sicherheitsrisiken senken, Aufgaben verteilen und die Effizienz erhöhen. Sie können vordefinierte Rollen verwenden oder eigene Rollen erstellen. |
| Integration des Unternehmensverzeichnisses | Sie können eine lokale, integrierte Benutzerauthentifizierung verwenden, um auf die Verwaltungskonsole und die Selbstbedienungskonsole zuzugreifen, oder Sie können die Authentifizierung in Microsoft Active Directory oder den in der Unternehmensumgebung verwendeten LDAP-Unternehmensverzeichnissen (beispielsweise IBM Domino Directory) integrieren. BlackBerry UEM unterstützt Verbindungen zu mehreren Verzeichnissen. Sie können eine beliebige Kombination von Microsoft Active Directory und LDAP verwenden.<br><br>Außerdem können Sie BlackBerry UEM so konfigurieren, dass die Mitgliedschaft einer mit einem Verzeichnis verknüpften Gruppe mit den zugehörigen Unternehmensverzeichnisgruppen automatisch synchronisiert wird, wenn die geplante Synchronisierung erfolgt.<br><br>Wenn Sie die Einstellungen für per Verzeichnis verknüpfte Gruppen konfigurieren, können Sie Offboarding-Schutz auswählen. Für den Offboarding-Schutz sind zwei unmittelbar aufeinander folgende Synchronisierungszyklen erforderlich, bevor Benutzerkonten oder Gerätedaten von BlackBerry UEM gelöscht werden. Diese Funktion hilft dabei, unerwartete Löschungen zu verhindern, die aufgrund von Latenz bei der Verzeichnisreplikation stattfinden können.<br><br>Zur Integration von BlackBerry UEM Cloud in Ihr Unternehmensverzeichnis müssen Sie BlackBerry Connectivity Node installieren. Sie können eine oder mehr Instanzen des BlackBerry Connectivity Node installieren. |
| Hohe Verfügbarkeit | Wenn Sie BlackBerry UEM Cloud verwenden, wartet BlackBerry den Dienst und maximiert die Laufzeit für Sie, sodass Sie Ihren eigenen hochverfügbaren Dienst zur Geräteverwaltung nicht mit allen damit verbundenen Laufzeit- und Wartungskosten selbst warten müssen. |

| Funktion | Beschreibung |
| --- | --- |
| Migration | Sie können Benutzer, Geräte, Gruppen und andere Daten von einer lokalen BlackBerry UEM-Quelldatenbank auf eine neue lokale oder BlackBerry UEM Cloud-Instanz migrieren. |
| Cisco ISE-Integration | Cisco Identity Services Engine (ISE) ist eine Software zur Netzwerkverwaltung, die einem Unternehmen die Möglichkeit bietet, den Zugriff von Geräten auf das Unternehmensnetzwerk zu steuern (z. B. Zugriff auf Wi-Fi- oder VPN-Verbindungen zulassen oder verweigern). Sie können eine Verbindung zwischen Cisco ISE und BlackBerry UEM (lokal) herstellen, damit Cisco ISE auf Daten von Geräten zugreifen kann, die auf BlackBerry UEM aktiviert sind. Cisco ISE prüft die Gerätedaten, um zu bestimmen, ob Geräte den Zugriffsrichtlinien Ihres Unternehmens entsprechen. |
| Regionale Bereitstellung | Sie können regionale Verbindungen für Unternehmensverbindungsfunktionen einrichten, indem Sie BlackBerry Connectivity Node-Instanzen in einer bestimmten Region bereitstellen. Dies wird auch als Servergruppe bezeichnet. Jeder BlackBerry Connectivity Node umfasst BlackBerry Secure Connect Plus, den BlackBerry Gatekeeping Service, den BlackBerry Secure Gateway, BlackBerry Proxy und den BlackBerry Cloud Connector. Sie können einer Servergruppe Profile für Unternehmensverbindungen und E-Mail-Funktionen zuordnen, sodass alle Benutzer, die eine Zuordnung dieser Profile aufweisen, eine bestimmte regionale Verbindung zur BlackBerry Infrastructure bei Verwendung von BlackBerry Connectivity Node-Komponenten nutzen. Durch die Bereitstellung von mehr als einem BlackBerry Connectivity Node in einer Servergruppe wird eine hohe Verfügbarkeit und Lastverteilung erzielt. |
| Wearable-Geräte | Sie können bestimmte Android-basierte, am Kopf tragbare Geräte in BlackBerry UEM aktivieren und verwalten. Zum Beispiel können Sie Vuzix M300 Smart Glasses verwalten. Intelligente Brillen ermöglichen den berührungslosen Zugriff auf visuelle Informationen, wie z. B. Benachrichtigungen, Schritt-für-Schritt-Anleitungen, Bilder und Videos, die Nutzung von Sprachsteuerung und GPS-Navigation oder das Scannen von Barcodes. Beispiele für BlackBerry UEM-Verwaltungsfunktionen, die unterstützt werden, umfassen: Geräteaktivierung mit QR-Code, IT-Richtlinien, Wi-Fi- und VPN-Profile, App-Management und standortbezogene Dienste. |

| Funktion | Beschreibung |
| --- | --- |
| Microsoft Intune-Integration | Für iOS- und Android-Geräte: Wenn Sie Daten in Microsoft Office 365-Apps mit den MAM-Funktionen von Microsoft Intune schützen wollen, können Sie Intune zum Schutz von App-Daten verwenden, während Sie BlackBerry UEM zur Verwaltung der Geräte nutzen. Intune bietet Sicherheitsfunktionen zum Schutz der Daten innerhalb von Apps. Zum Beispiel kann Intune erfordern, dass Daten innerhalb von Apps verschlüsselt werden, und das Kopieren und Einfügen, Drucken und die Verwendung des Befehls „Speichern unter“ verhindern. Sie können UEM mit Intune verbinden, sodass Sie Intune-App-Sicherheitsrichtlinien über die UEM-Verwaltungskonsole verwalten können. |

# Schlüsselmerkmale aller Gerätetypen

Es stehen Aktivitäten zur Verfügung, die Sie mit allen von BlackBerry UEM unterstützten Gerätetypen durchführen können. Hierzu zählen die Aktivierung von Geräten, die Verwaltung von Geräten, Apps und Lizenzen, die Steuerung, wie die Geräte eine Verbindung zu den Ressourcen in Ihrem Unternehmen herstellen, und die Durchsetzung der Anforderungen des Unternehmens. Weitere Informationen zu diesen Funktionen finden Sie in der folgenden Tabelle.

| Funktion | Beschreibung |
|---|---|
| Aktivieren von Geräten | Wenn Sie ein Gerät aktivieren, weisen Sie das Gerät Ihrer Unternehmensumgebung zu, damit Benutzer auf ihren Geräten auf Geschäftsdaten zugreifen können. Sie können ein Gerät einfach nur mit einer E-Mail-Adresse und einem Aktivierungskennwort aktivieren.<br><br>Sie können Benutzern erlauben, dass sie selbst Geräte aktivieren, oder Sie können die Geräte für die Benutzer aktivieren und anschließend verteilen. Alle Gerätetypen können über das Mobilfunknetz aktiviert werden. |
| Geräte verwalten | Sie können alle Geräte an einem Ort anzeigen und alle Verwaltungsaufgaben über eine einzelne webbasierte Benutzerschnittstelle aufrufen. Sie können mehrere Geräte für jedes Benutzerkonto verwalten und den Gerätbestand Ihres Unternehmens anzeigen. Sie können die folgenden Aktionen durchführen, sofern diese vom Gerät unterstützt werden:<br><br>• Sperren des Geräts, Ändern des Kennworts für das Gerät bzw. für den geschäftlichen Bereich oder Löschen der Informationen vom Gerät<br>• Sicheres Verbinden des Geräts mit der E-Mail-Umgebung Ihres Unternehmens durch Verwendung von Microsoft Exchange ActiveSync zur Unterstützung von E-Mail und Kalender<br>• Steuern, wie das Gerät auf das Unternehmensnetzwerk, einschließlich Wi-Fi und VPN-Einstellungen, zugreifen kann<br>• Konfigurieren der einmaligen Anmeldung für das Gerät, sodass es sich automatisch bei Domänen und Webdiensten innerhalb Ihres Unternehmensnetzwerks authentifiziert<br>• Steuern der Funktionen des Geräts, u. a. Einrichten von Regeln für die Kennwortsicherheit und Deaktivieren von Funktionen, z. B. die Kamera<br>• Verwalten der App-Verfügbarkeit auf dem Gerät, einschließlich der Angabe von App-Versionen und ob die Apps obligatorisch oder optional sind<br>• Durchsuchen von App Stores direkt nach Apps, die Geräten zugewiesen werden können<br>• Installieren von Zertifikaten auf dem Gerät und optionales Konfigurieren von SCEP, um die automatische Zertifikatsanmeldung zuzulassen<br>• Erweitern der E-Mail-Sicherheit mithilfe von S/MIME oder PGP |
| Verwalten von Benutzergruppen, Apps und Geräten | Mithilfe von Gruppen wird die Verwaltung von Benutzern, Apps und Geräten vereinfacht. Sie können Gruppen dazu verwenden, um die gleichen Konfigurationseinstellungen auf ähnliche Benutzerkonten oder Geräte anzuwenden. Sie können unterschiedliche App-Gruppen zu verschiedenen Benutzergruppen zuweisen, und ein Benutzer kann Mitglied mehrerer Gruppen sein. |

| Funktion | Beschreibung |
| --- | --- |
| Steuern, welche Geräte Zugriff auf Microsoft Exchange ActiveSync erhalten | Mit Gatekeeping in BlackBerry UEM können Sie sicherstellen, dass nur von BlackBerry UEM verwaltete Geräte auf die geschäftliche E-Mail und andere Informationen auf dem Gerät zugreifen können und dass die Sicherheitsrichtlinie Ihres Unternehmens eingehalten wird. |
| Steuern, wie Geräte auf die Unternehmensressourcen zugreifen | Mithilfe eines Enterprise-Konnektivitäts-Profils können Sie steuern, wie Apps auf Geräten eine Verbindung mit den Ressourcen Ihres Unternehmens herstellen. Wenn Sie die Enterprise-Konnektivität aktivieren, vermeiden Sie das Öffnen mehrerer Ports in Ihrer Firewall zum Internet zur Geräteverwaltung oder zu Drittanbieteranwendungen, wie dem E-Mail-Server, der Zertifizierungsstelle und anderen Web- oder Inhaltsservern. Die Enterprise-Konnektivität sendet den gesamten Datenverkehr über die BlackBerry Infrastructure an BlackBerry UEM an Port 3101. |
| Verwalten von geschäftlichen Apps | Auf allen verwalteten Geräten sind geschäftliche Apps solche, die den Benutzern von Unternehmen zur Verfügung gestellt werden.<br><br>Sie können App Stores direkt nach Apps durchsuchen, die Geräten zugewiesen werden sollen. Sie können angeben, ob Apps auf Geräten erforderlich sind, und Sie können sehen, ob eine geschäftliche App auf einem Gerät installiert ist. Geschäftliche Apps können auch firmeneigene Apps sein, die speziell von Ihrem Unternehmen oder von Drittentwicklern zur Verwendung durch Ihr Unternehmen entwickelt wurden. |
| Durchsetzung der Anforderungen Ihres Unternehmens für Geräte | Mithilfe eines Profils für die Vorschrifteneinhaltung können Sie dazu beitragen, dass die Anforderungen Ihres Unternehmens an Geräte durchgesetzt werden. Beispielsweise können Sie den Zugriff auf geschäftliche Daten durch Geräte, die entsperrt oder gehackt wurden oder für die ein Integritätsalarm vorliegt, unterbinden oder die Installation bestimmter Apps auf Geräten erzwingen. Sie können Benutzern eine Benachrichtigung senden und sie auffordern, die Anforderungen Ihres Unternehmens zu erfüllen. Sie können auch den Zugriff von Benutzern auf die Ressourcen und Anwendungen Ihres Unternehmens beschränken und Geschäftsdaten oder alle Daten auf dem Gerät löschen. |
| Senden einer E-Mail an Benutzer | Sie können direkt über die Verwaltungskonsole E-Mail-Nachrichten an mehrere Benutzer senden. Die Benutzer müssen über ein Konto mit einer verknüpften E-Mail-Adresse verfügen. |
| Erstellen oder Importieren von vielen Benutzerkonten mit einer .csv-Datei | Sie können eine .csv-Datei in BlackBerry UEM importieren, um viele Benutzerkonten gleichzeitig zu erstellen oder zu importieren. Bei Bedarf können Sie in der .csv-Datei auch Gruppenmitgliedschaften und Aktivierungseinstellungen angeben. |
| Anzeigen von Berichten mit Benutzer- und Geräteinformationen | Im Berichts-Dashboard wird ein Überblick über Ihre BlackBerry UEM-Umgebung angezeigt. Beispielsweise können Sie die Anzahl der Geräte Ihres Unternehmens nach dem Dienstanbieter sortiert anzeigen. Sie können Einzelheiten zu Benutzern und Geräten anzeigen und in eine .csv-Datei exportieren sowie vom Dashboard aus auf die Benutzerkonten zugreifen. |

| Funktion | Beschreibung |
| --- | --- |
| Hohe Verfügbarkeit und Notfallwiederherstellung für die BlackBerry Infrastructure und BlackBerry UEM Cloud-Umgebungen | BlackBerry-Rechenzentren sind auf der ganzen Welt verteilt und wurden so entwickelt, dass sie Hochverfügbarkeit und Notfallwiederherstellungskapazitäten bieten. BlackBerry-Datencenter bieten einen äußerst sicheren physischen Zugriff auf Gebäude, Überwachungsfunktionen und Hardwareredundanzen, um die Daten Ihres Unternehmens vor Naturkatastrophen und nicht autorisiertem Zugriff zu schützen.<br>BlackBerry-Rechenzentren verfügen über Pläne zur Notfallwiederherstellung bei Ausfällen von Diensten. Die Pläne sind so konzipiert, dass sie eine minimale Auswirkung auf die Benutzer der Geräte haben und dass die Kontinuität des Geschäfts sichergestellt wird. Daten und Anwendungen werden nahezu in Echtzeit gesichert, um Datenverlust zu vermeiden. |
| Zertifikatsbasierte Authentifizierung | Sie können Zertifikate mithilfe von Zertifikatsprofilen an Geräte senden. Diese Profile helfen dabei, den Zugriff auf Microsoft Exchange ActiveSync-, Wi-Fi- oder VPN-Verbindungen auf Geräte zu beschränken, die eine zertifikatsbasierte Authentifizierung nutzen. |
| Verwalten von Lizenzen für bestimmte Funktionen und Gerätesteuerungen | Sie können für die einzelnen Lizenztypen die Lizenzen verwalten und detaillierte Informationen anzeigen, wie etwa zu Nutzungs- und Ablaufdaten. Durch die von Ihrem Unternehmen verwendeten Lizenztypen werden die Geräte und Funktionen bestimmt, die Sie verwalten können. Sie müssen Lizenzen aktivieren, bevor Sie Geräte aktivieren können. Es stehen kostenlose Testversionen zur Verfügung, sodass Sie den Dienst ausprobieren können. |

# Schlüsselmerkmale der einzelnen Gerätetypen

**iOS-Geräte**

| Funktion | Beschreibung |
|---|---|
| Verwenden des App-Sperrmodus | Sie können mithilfe eines Profils für den App-Sperrmodus auf iOS-Geräten, die mit Apple Configurator 2 überwacht werden, festlegen, dass nur eine App ausgeführt wird. Beispielsweise können Sie ein Gerät zu Schulungszwecken oder für Vorführungen am Verkaufsort auf eine einzige App beschränken. |
| Geräteaktivierung | Mit dem Apple Configurator 2 können Geräte für die Aktivierung in BlackBerry UEM vorbereitet werden. Benutzer können die vorbereiteten Geräte aktivieren, ohne die BlackBerry UEM Client-App verwenden zu müssen. |
| Filtern von Webinhalten | Sie können mithilfe von Webinhaltsfilter-Profilen die Webseiten einschränken, die ein Benutzer auf einem Gerät aufrufen kann. Sie können das automatische Filtern mit der Option zum Zulassen und Einschränken von Websites aktivieren oder den Zugriff nur auf bestimmte Websites zulassen. |
| Verknüpfen von Apple VPP-Konten mit einer BlackBerry UEM-Domäne | VPP (Volume Purchase Program) ermöglicht Ihnen, iOS-Apps in Mengen zu kaufen und zu verteilen. Sie können Apple VPP-Konten mit einer BlackBerry UEM-Domäne verknüpfen, sodass Sie gekaufte Lizenzen für mit VPP-Konten verknüpfte iOS-Apps verteilen können. |
| Programm zur Geräteregistrierung (DEP) von Apple | Sie können BlackBerry UEM für die Verwendung des Programms zur Geräteregistrierung (DEP) von Apple konfigurieren, damit Sie BlackBerry UEM mit DEP synchronisieren können. Nach der Konfiguration von BlackBerry UEM können Sie die Aktivierung der von Ihrem Unternehmen für DEP erworbenen iOS-Geräte mit der BlackBerry UEM-Verwaltungskonsole verwalten. Sie können mehrere DEP-Konten verwenden.<br><br>Sie können mehrere Apple-DEP-Konten mit einer BlackBerry UEM-Domäne verknüpfen. |
| Unterstützung für App-basierte PKI-Lösungen | Zusätzliche Unterstützung für App-basierte PKI-Lösungen wie Purebred zur Registrierung von Zertifikaten für BlackBerry Dynamics-Apps. Sie können die PKI-App jetzt auf Geräten installieren und den aktuellen Versionen von BlackBerry Dynamics-Apps wie BlackBerry Work und BlackBerry Access erlauben, über die PKI-App registrierte Zertifikate zu verwenden. |
| Verwenden benutzerdefinierterPayload-Profile | Mit benutzerdefinierten Payload-Profilen können Sie Funktionen auf iOS-Geräten steuern, die nicht durch bestehende BlackBerry UEM-Richtlinien oder -Profile gesteuert werden. Sie können mit Apple Configurator Apple-Konfigurationsprofile erstellen und diese den benutzerdefinierten BlackBerry UEM-Payload-Profilen hinzufügen. Sie können benutzerdefinierte Payload-Profile Benutzern, Benutzergruppen und Gerätegruppen zuweisen. |

| Funktion | Beschreibung |
| --- | --- |
| BlackBerry Secure Gateway | Der BlackBerry Secure Gateway ermöglicht iOS-Geräten mit der Aktivierungsart „MDM-Steuerelemente“ die Verbindung zu einem geschäftlichen E-Mail-Server über die BlackBerry Infrastructure und BlackBerry UEM. Wenn Sie den BlackBerry Secure Gateway verwenden, müssen Sie Ihren E-Mail-Server nicht außerhalb der Firewall verfügbar machen, damit Benutzer dieser Geräte geschäftliche E-Mails empfangen können, wenn keine Verbindung zum VPN Ihres Unternehmens oder dem geschäftlichen Wi-Fi-Netzwerk besteht. |
| Integration mit BlackBerry Dynamics | Sie können das BlackBerry Dynamics-Profil verwenden, um iOS-Geräten den Zugriff auf BlackBerry Dynamics-Produktivität-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect zu ermöglichen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen das BlackBerry Dynamics-Profil zuweisen. Mehrere Geräte können auf dieselben Apps zugreifen.<br>Das Profil ermöglicht die Aktivierung von BlackBerry Dynamics für Benutzer, die noch nicht für BlackBerry Dynamics aktiviert sind. |
| Per-App-VPN | Sie können ein Per-App-VPN für iOS-Geräte einrichten, um anzugeben, welche Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Ein Per-App-VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (z. B. Zugriff auf Anwendungsserver oder Webseiten hinter der Firewall). Diese Funktion unterstützt auch die Privatsphäre des Benutzers und erhöht die Verbindungsgeschwindigkeit für persönliche Apps, indem der persönliche Datenverkehr nicht über das VPN gesendet wird.<br>Für iOS-Geräte sind Apps mit einem VPN-Profil verknüpft, wenn Sie die App oder App-Gruppe einem Benutzer, einer Benutzergruppe oder einer Gerätegruppe zuweisen. |
| Apple-Aktivierungssperre | Für die Funktion „Aktivierungssperre“ sind Apple-ID und Kennwort des Benutzers erforderlich, bevor ein Benutzer „Mein iPhone suchen“ deaktivieren, das Gerät löschen oder reaktivieren und verwenden kann. Sie können die Aktivierungssperre umgehen, um ein COPE- oder COBO-Gerät einem anderen Benutzer zur Verfügung zu stellen. |
| Persönliche App-Listen | Sie können eine Liste der Apps anzeigen, die im persönlichen Bereich des Benutzers auf iOS-Geräten in Ihrer Umgebung installiert sind. Sie können über die Seite „Benutzerdetails“ eine Liste der auf dem Gerät eines Benutzers installierten persönlichen Apps anzeigen, oder Sie können über die Seite „Persönliche Apps“ in der Verwaltungskonsole eine Liste aller persönlichen Apps anzeigen, die in persönlichen Bereichen der Benutzer installiert sind. |
| Verloren-Modus für überwachte iOS-Geräte | Der Verloren-Modus ermöglicht das Sperren eines Geräts, das Festlegen einer anzuzeigenden Nachricht und das Anzeigen des aktuellen Standorts eines verloren gegangenen Geräts. Sie können den Verloren-Modus für überwachte iOS-Geräte aktivieren. |
| IBM Notes Traveler-Unterstützung | iOS-Geräte können eine Verbindung zu IBM Notes Traveler über den BlackBerry Secure Gateway herstellen. |

| Funktion | Beschreibung |
| --- | --- |
| Face ID-Unterstützung | BlackBerry UEM unterstützt die Face ID für die Authentifizierung von Geräten und zum Öffnen von BlackBerry Dynamics-Apps. |
| Verwaltung freigegebener Geräte | Sie können zulassen, dass mehrere Benutzer ein iOS-Gerät gemeinsam verwenden. Sie können die Nutzungsbestimmungen anpassen, die Benutzer akzeptieren müssen, um freigegebene Geräte abzumelden. Ein Benutzer kann ein Gerät per lokaler Authentifizierung abmelden und sobald er fertig ist wieder anmelden, damit es für den nächsten Benutzer zur Verfügung steht. Freigegebene Geräte werden während des Abmeldungs- und Anmeldungsprozesses von BlackBerry UEM verwaltet. Diese Funktion wurde speziell für überwachte Geräte mit der folgenden Konfiguration entwickelt:<br>• App-Sperrmodus aktiviert<br>• VPP-Apps zugewiesen |

**Android-Geräte**

| Funktion | Beschreibung |
| --- | --- |
| Android Enterprise-Geräte verwalten | Sie können Android-Geräte für die Verwendung von Android Enterprise aktivieren. Diese Funktion wurde von Google entwickelt und bietet zusätzliche Sicherheit für Unternehmen, die Android-Geräte verwalten und ihre Daten und Apps auf Android-Geräten zulassen wollen.<br>Geräte können so aktiviert werden, dass sie nur ein geschäftliches oder sowohl ein geschäftliches als auch ein persönliches Profil haben. Sie haben die volle Kontrolle über beide Profile und können das gesamte Gerät löschen. Sie können dem Benutzer aber auch für das persönliche Profil Privatsphäre gewähren und sich nur für die geschäftlichen Daten auf dem Gerät Löschrechte vorbehalten.<br>Samsung und BlackBerry auf Android-Geräten bieten zusätzliche Administratoroptionen, unter anderem auch (bei einer Aktivierung mit Android Enterprise) erweiterte IT-Richtlinienregeln. |
| Aktivierungen für Android Enterprise-Geräte: „Geschäftlich und persönlich – vollständige Kontrolle“ | Dieser Aktivierungstyp gilt für Geräte mit Android 8 oder höher. Sie können damit das gesamte Gerät verwalten. Es wird ein Arbeitsprofil auf dem Gerät erstellt, das geschäftliche und persönliche Daten trennt, Ihrer Organisation jedoch die vollständige Kontrolle über das Gerät und die Möglichkeit einer Bereinigung aller Daten auf dem Gerät sichert. Sowohl die Daten im geschäftlichen als auch im persönlichen Profil werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise ein Kennwort, geschützt. |

| Funktion | Beschreibung |
| --- | --- |
| Verwalten von Geräten mit Knox MDM und Knox Workspace | BlackBerry UEM kann Samsung-Geräte mithilfe von Samsung Knox MDM und Samsung Knox Workspace verwalten. Knox Workspace bietet einen verschlüsselten kennwortgeschützten Container auf einem Samsung-Gerät für geschäftliche Apps und Daten. Er trennt die persönlichen Apps und Daten eines Benutzers von denen des Unternehmens und schützt letztere mithilfe erweiterter, von Samsung entwickelter Sicherheits- und Verwaltungsfunktionen.<br><br>Wenn ein Gerät aktiviert wird, erkennt BlackBerry UEM automatisch, ob das Gerät Knox unterstützt. Zusätzlich zu den Standard-Verwaltungsfunktionen für Android bietet BlackBerry UEM die folgenden Verwaltungsfunktionen für Geräte, die Knox unterstützen:<br><br>• Erweiterte IT-Richtlinienregeln<br>• Erweiterte Anwendungsverwaltung, einschließlich automatischer Installation und Deinstallation von Apps, automatischer Deinstallation gesperrter Apps und Verhinderung der Installation gesperrter Apps<br>• App-Sperrmodus<br><br>Weitere Informationen zu den unterstützten Geräten finden Sie in der Kompatibilitätsmatrix. Weitere Informationen zu Knox finden Sie unter https://www.samsungknox.com. |
| Integration mit BlackBerry Dynamics | Sie können das BlackBerry Dynamics-Profil verwenden, um Android-Geräten den Zugriff auf BlackBerry Dynamics-Produktivität-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect zu ermöglichen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen das BlackBerry Dynamics-Profil zuweisen. Mehrere Geräte können auf dieselben Apps zugreifen.<br><br>Das Profil ermöglicht die Aktivierung von BlackBerry Dynamics für Benutzer, die noch nicht für BlackBerry Dynamics aktiviert sind. |
| Per-App-VPN | Sie können „Per App VPN“ für Android-Geräte mit Arbeitsprofil aktivieren, um die Verwendung von BlackBerry Secure Connect Plus auf bestimmte geschäftliche Apps zu beschränken, die Sie einer Positivliste hinzufügen. |
| Zero-Touch-Registrierung | BlackBerry UEM unterstützt Geräte mit Android 8.0 oder höher, auf denen die Zero-Touch-Registrierung aktiviert wurde. Die Zero-Touch-Registrierung bietet eine nahtlose Bereitstellungsmethode für Android-Geräte in Unternehmensbesitz und ermöglicht eine schnelle, einfache und sichere Gerätebereitstellung für Unternehmen und Mitarbeiter. Die Zero-touch-Registrierung macht es IT-Administratoren einfach, Geräte online zu konfigurieren und ihre Verwaltung durchzusetzen, wenn Mitarbeiter ihre Geräte bekommen. Siehe Google: Verwaltung der Zero-Touch-Registrierung und Überblick über die Zero-Touch-Registrierung. Sie können die Zero-Touch-Registrierung in nur wenigen Schritten aktivieren: Geräte kaufen, Geräte den Benutzern zuweisen, Richtlinien für Ihr Unternehmen konfigurieren und den Benutzern die Geräte bereitstellen. Sie müssen mit Ihrem Händler oder Anbieter zusammenarbeiten, um Zugriff auf das Zero-Touch-Portal zu erhalten und Geräte im Portal zu konfigurieren. |

| Funktion | Beschreibung |
| --- | --- |
| Unterstützung für App-basierte PKI-Lösungen | Unterstützung für App-basierte PKI-Lösungen wie Purebred zur Registrierung von Zertifikaten für BlackBerry Dynamics-Apps. Sie können die PKI-App auf Geräten installieren und den aktuellen Versionen von BlackBerry Dynamics-Apps wie BlackBerry Work und BlackBerry Access erlauben, über die PKI-App registrierte Zertifikate zu verwenden. |
| Android SafetyNet | Wenn Administratoren Android SafetyNet-Nachweise aktivieren, sendet BlackBerry UEM Anforderungen zum Testen der Authentizität und der Integrität von Android-Geräten, die mit den Aktivierungsarten Android Enterprise, Samsung Knox und MDM-Steuerelementen in Ihrer Unternehmensumgebung aktiviert wurden. |
| Durchsetzung von Sicherheitspatchstufen für BlackBerry Dynamics-Apps | Sie können die Durchsetzung von Sicherheitspatches auf BlackBerry Dynamics-Apps anwenden. Wenn die Sicherheitspatchstufe nicht erfüllt ist, können Sie die BlackBerry Dynamics-App-Daten löschen, die Ausführung von BlackBerry Dynamics-Apps auf dem Gerät nicht zulassen oder keine Aktionen auf dem Gerät ausführen. |
| Abgeleitete Smart Credentials | Verwenden Sie von Entrust IdentityGuard abgeleitete iSmart Credentials zur Signatur, Verschlüsselung und Authentifizierung für BlackBerry Dynamics-Apps und Apps im geschäftlichen Bereich von Android Enterprise- und Samsung Knox Workspace-Geräten. |
| Schutz bei Zurücksetzen auf die Werkseinstellungen für Android Enterprise-Geräte | Sie können für die Android Enterprise-Geräte Ihres Unternehmens, bei denen nur der geschäftliche Bereich aktiviert ist, ein Schutzprofil für den Fall, dass sie auf die Werkseinstellungen zurückgesetzt werden, anlegen. Mit diesem Profil können Sie ein Benutzerkonto festlegen, mit dem ein Gerät entsperrt werden kann, nachdem es auf die Werkseinstellungen zurückgesetzt wurde, oder nach einem Zurücksetzen auf die Werkseinstellungen den Zugriff ohne Zugangsdaten gestatten. |

#### Windows 10-Geräte

| Funktion | Beschreibung |
| --- | --- |
| Unterstützung für Windows 10-Geräte | Sie können Windows 10-Geräte – Windows 10-Mobilgeräte und Windows 10-Tablets und -Computer – verwalten. |
| Proxyunterstützung für Windows 10-Geräte | Sie können VPN- und geschäftliche WLAN-Verbindungen für Windows 10-Geräte konfigurieren und einen Proxyserver als Teil des Wi-Fi-Profils Windows 10 Mobile- für Geräte einrichten. |

| Funktion | Beschreibung |
| --- | --- |
| Per-App-VPN | Sie können ein Per-App-VPN für Windows 10-Geräte einrichten, um anzugeben, welche Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Ein Per-App-VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (z. B. Zugriff auf Anwendungsserver oder Webseiten hinter der Firewall). Diese Funktion unterstützt auch die Privatsphäre des Benutzers und erhöht die Verbindungsgeschwindigkeit für persönliche Apps, indem der persönliche Datenverkehr nicht über das VPN gesendet wird.<br><br>Für Windows 10-Geräte werden im VPN-Profil Apps der App-Auslöserliste hinzugefügt. |
| Windows-Datenschutz für Windows 10-Geräte | Sie können Windows-Datenschutzprofile konfigurieren, um persönliche Daten und geschäftliche Daten auf Geräten getrennt voneinander zu halten, um Benutzer daran zu hindern, geschäftliche Daten außerhalb von geschützten geschäftlichen Apps freizugeben oder mit Personen außerhalb des Unternehmens zu teilen und um unangemessene Methoden zum Teilen von Daten zu überwachen. Sie können angeben, welche Apps geschützt sind und welchen Apps vertraut wird, um geschäftliche Dateien zu erstellen und darauf zuzugreifen. |
| Whitelist für Virenschutzanbieter | Im Konformitätsprofil können Sie in der Regel „Antivirus-Status“ für Windows-Geräte festlegen, dass Antivirensoftware entweder von beliebigen Herstellern zugelassen wird, oder nur von solchen, die Sie der Liste „Zulässige Virenschutzanbieter“ hinzugefügt haben. Die Regel wird dann durchgesetzt, wenn auf einem Gerät Virenschutzsoftware von einem anderen, nicht in der Whitelist aufgeführten Anbieter aktiviert ist. |
| Azure Active Directory Join | BlackBerry UEM unterstützt Azure Active Directory Join, um den MDM-Registrierungsvorgang für Windows 10-Geräte zu vereinfachen. Benutzer können ihre Geräte mit BlackBerry UEM unter Zuhilfenahme ihres Azure Active Directory-Benutzernamens und -Kennworts registrieren. Azure Active Directory unterstützt außerdem Windows AutoPilot, sodass Windows 10-Geräte während dem Out-of-the-Box-Experience in Windows 10 automatisch mit BlackBerry UEM aktiviert werden können. **Hinweis**: Um die automatische MDM-Registrierung mit BlackBerry UEM während der Windows 10-Out-of-the-Einrichtung zu aktivieren, muss auf dem Gerät ein BlackBerry UEM-Zertifikat installiert sein. |

**BlackBerry 10-Geräte**

| Funktion | Beschreibung |
| --- | --- |
| Getrenntes Verwalten von geschäftlichen Informationen auf BlackBerry 10-Geräten | Durch die BlackBerry Balance-Technologie wird sichergestellt, dass persönliche und geschäftliche Informationen und Apps auf BlackBerry 10-Geräten getrennt gehalten werden. Sie erstellt einen persönlichen und einen geschäftlichen Bereich und bietet umfassende Verwaltungsfunktionen für den geschäftlichen Bereich. Für staatliche und gesetzlich geregelte Branchen, die das Gerät noch sicherer machen möchten, gibt es zusätzliche Optionen, die die vollständige Steuerung des geschäftlichen Bereichs und die teilweise Steuerung des persönlichen Bereichs gewähren. Alternativ haben Sie die Möglichkeit, lediglich einen geschäftlichen Bereich auf dem Gerät zu erstellen, sodass Ihr Unternehmen die volle Kontrolle über das Gerät erhält. |

# Kompatibilität und Anforderungen

Sie finden die aktuellsten Informationen zur Kompatibilität von Gerätetypen, Betriebssystemen für Geräte, Browsern usw. für den Zugriff auf BlackBerry UEM in der BlackBerry UEM-Kompatibilitätsmatrix.

# Rechtliche Hinweise



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

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

SOFERN ES NICHT DURCH DAS IN IHREM RECHTSGEBIET GELTENDE RECHT AUSDRÜCKLICH UNTERSAGT IST, WERDEN HIERMIT SÄMTLICHE AUSDRÜCKLICHEN ODER KONKLUDENTEN BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN JEDER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF BEDINGUNGEN, BILLIGUNGEN, GARANTIEN, ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN HINSICHTLICH DER HALTBARKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER VERWENDUNGSZWECK, MARKTGÄNGIGKEIT, MARKTGÄNGIGEN QUALITÄT, NICHTVERLETZUNG VON RECHTEN DRITTER, ZUFRIEDENSTELLENDEN QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, CHANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDEN LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTPRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE GELTEN FÜR SIE ZUDEM ANDERE LANDESSPEZIFISCHE RECHTE. IN MANCHEN RECHTSGEBIETEN IST DER AUSSCHLUSS ODER DIE EINSCHRÄNKUNG KONKLUDENTER GEWÄHRLEISTUNGEN UND BEDINGUNGEN NICHT ZULÄSSIG. IN DEM GESETZLICH ZULÄSSIGEN UMFANG WERDEN SÄMTLICHE KONKLUDENTEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN IM ZUSAMMENHANG MIT DER DOKUMENTATION, DIE EINGESCHRÄNKT WERDEN KÖNNEN, SOFERN SIE NICHT WIE OBEN DARGELEGT AUSGESCHLOSSEN WERDEN KÖNNEN, HIERMIT AUF 90 TAGE AB DATUM DES ERWERBS DER DOKUMENTATION ODER DES ARTIKELS, AUF DEN SICH DIE FORDERUNG BEZIEHT, BESCHRÄNKT.

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

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

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

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

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

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

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

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

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
Großbritannien

Veröffentlicht in Kanada