



BlackBerry UEM

Versionshinweise und Ratgeber

12.12

Contents

Installieren der Software..... 4

Neuerungen in BlackBerry UEM 12.12..... 5

Behobene Probleme..... 24

Bekannte Probleme in BlackBerry UEM 12.12..... 25

Rechtliche Hinweise..... 29

Installieren der Software

Sie können mithilfe der Setupanwendung die Version BlackBerry UEM 12.12 installieren oder ein Upgrade von 12.10.x oder 12.11.x durchführen. Wenn Sie ein Upgrade der Software durchführen, werden alle BlackBerry UEM-Dienste von der Setupanwendung beendet und neu gestartet. Die BlackBerry UEM-Setupanwendung erstellt automatisch eine Sicherungskopie der Datenbank.

Hinweis: Ab Version BlackBerry UEM 12.10 ist JRE nicht mehr im Umfang des Installationsprogramms enthalten. Wenn Sie BlackBerry UEM installieren, müssen Sie zunächst JRE herunterladen und installieren (mindestens Version JRE 8u151).

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 herstellereigenen 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-Verknüpfungsfiler:** 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-Steurelemente	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-Steurelemente	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-Steurelemente	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-Steurelemente	Ausgewählt
iOS	Gerätefunktionalität	Aktivierung von Wi-Fi erzwingen	Legen Sie fest, ob Wi-Fi auf dem Gerät	MDM-Steurelemente	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	Sperrbildschirmmeldeanfordern	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	Sperrbildschirm	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 Gerätekenntwort zulässig ist. Gilt nur, wenn die Qualität des Gerätekenntworts 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. 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 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	

Behobene Probleme

Behobene Probleme bei Installation, Upgrade und Migration

Sie konnten kein Upgrade von UEM 12.9 auf UEM 12.11 durchführen, wenn der Verzeichnispfad Klammern enthielt. Beispiel: C:\Program Files (EXAMPLE)\BlackBerry\UEM\ (JI 2737983)

Behobene Probleme bei der Benutzer- und Geräteverwaltung

Wenn Sie ein vorhandenes App-Sperrmodus-Profil für ein Samsung Knox-Gerät geändert haben, wurde das aktualisierte Profil auf dem Gerät nicht korrekt aktualisiert. (JI 2768251)

Sie konnten Enterprise-Konnektivitätsprofile nicht ändern und speichern, für die iOS-VPN-On-Demand-Regeln konfiguriert waren. (JI 2773122)

Bekannte Probleme mit der Verwaltungskonsole

Wenn Sie im Abschnitt „Apps“ der BlackBerry UEM-Verwaltungskonsole eine App-Kategorie ausgewählt und dann eine Suche nach den gefilterten Ergebnissen durchgeführt haben, wurden die App-Kategorien nach der Suche nicht mehr angezeigt. (JI 2763761)

Wenn eine DEP-Verbindung fehlgeschlagen ist, weil ein neues Token im Apple-DEP-Portal generiert wurde, haben Sie keine Ereignisbenachrichtigung per E-Mail erhalten. (JI 2741015)

Wenn Sie auf „Verwaltete Geräte“ oder „Alle Benutzer“ geklickt, einen Benutzer ausgewählt, die Größe des Fensters geändert und auf den Zurück-Pfeil geklickt haben, wurde ein leerer Bildschirm angezeigt. (JI 2734658)

Es wurde keine Warnmeldung angezeigt, wenn Sie ein Aktivierungsprofil für ein Android-Gerät erstellt und keinen Aktivierungstyp ausgewählt haben. (JI 2716799)

Bekannte Probleme in BlackBerry UEM 12.12

Elemente, die mit einem Sternchen (*) markiert sind, sind seit dieser Version bekannt.

Bekannte Probleme bei Installation, Upgrade und Migration

* BlackBerry Secure Connect Service wird nach einem Software-Upgrade möglicherweise nicht gestartet. (JI 2810236)

Problemumgehung: Führen Sie das Upgrade erneut aus.

Wenn Sie das BlackBerry Workspaces-Plug-in mit BlackBerry UEM installieren und dann die UEM-Verwaltungskonsole öffnen, wird eine Fehlermeldung angezeigt, obwohl BlackBerry UEM und BlackBerry Workspaces das erwartete Verhalten zeigen. (JI 2758927)

Problemumgehung: Schließen Sie die Fehlermeldung. Sie wird nicht erneut angezeigt.

Wenn Sie Apps von Good Control zu BlackBerry UEM migrieren und keine Richtlinie mit einem Authentifikator in Good Control konfiguriert haben, BlackBerry UEM jedoch über eine Richtlinie verfügt, die App A als Authentifikator konfiguriert, und Sie App B migrieren, wird die Migration der App blockiert, weil App A nicht migriert wurde. Wenn Sie anschließend App A migrieren, bleibt App B weiterhin blockiert, weil keine Anfrage an App A gesendet wird, um festzustellen, ob sie migriert wurde. (JI 2507114)

Problemumgehung: Erzwingen Sie auf dem Gerät das Stoppen der Apps, und starten Sie App B anschließend neu.

Bekannte Probleme bei der Benutzer- und Geräteverwaltung

Beachten Sie, dass einige dieser Probleme für BlackBerry UEM Client gelten und in einer zukünftigen Version von BlackBerry UEM Client behoben werden.

* Die Meldung „Neue Apps sind verfügbar“ wird möglicherweise nicht auf Android-Geräten ohne Google Play-Konto angezeigt, die mit der Aktivierungsart „Nur geschäftlicher Bereich (Android Enterprise)“ aktiviert wurden. (JI 2811290)

Problemumgehung: Benutzer können im BlackBerry UEM Client auf geschäftliche Apps tippen, um zu prüfen, ob neue Apps verfügbar sind.

* Apps von Benutzern können nicht auf der Registerkarte „<x> Benutzern zugewiesen“ entfernt werden. (JI 2802278)

Problemumgehung: Gehen Sie zur Seite des Benutzers, und löschen Sie die App.

* Wenn Sie Internet Explorer 11 verwenden und die erweiterte Sicherheitskonfiguration aktiviert ist, können Sie keinen BlackBerry Router hinzufügen oder bearbeiten. (JI 2802222)

* Wenn Sie eine Liste genehmigter Geräte-IDs für Android-Geräte konfiguriert, die Option „Nur genehmigte Geräte-IDs zulassen“ in Ihrem Aktivierungsprofil ausgewählt und dann ein Android-Gerät aktiviert haben, das nicht in der genehmigten Liste enthalten war, schlug die Aktivierung nicht fehl. (JI 2799509)

Zertifikate aus einem Entrust-Profil mit zwei Schlüsselpaaren können nicht auf einem iOS-Gerät installiert werden. (JI 2662697)

Auf einem Gerät mit Android 9, wenn die Sicherheitsrichtlinien-Einstellung zum Verhindern von Bildschirmaufnahmen deaktiviert ist, kann der Benutzer Daten von einer BlackBerry Dynamics-App in eine Nicht-BlackBerry Dynamics-App ausschneiden/darin kopieren/freigeben, auch wenn der Schutz vor Datenverlust (DLP) über die Pixel Launcher-Funktion aktiviert ist. Um Datenverluste zu verhindern, wird empfohlen, dass Sie die Richtlinieneinstellung zum Verhindern von Bildschirmaufnahmen aktivieren. (JI 2598556)

Sie können die Purebred-App und Entrust Smart Credentials nicht gleichzeitig auf iOS-Geräten mit BlackBerry Dynamics verwenden. Wenn Sie dies tun, wird das Purebred-Zertifikat in das falsche Profil für Benutzeranmeldeinformationen importiert. (JI 2585322)

Wenn Ihre Organisation PKI und Entrust Smart Credentials zusammen verwendet, müssen Benutzer das PKI-Zertifikat möglicherweise mehrmals auf dem gleichen Gerät anmelden (maximal einmal pro App). (JI 2580228)

Die Option „Android-Sprachaufzeichnung nicht zulassen“ im BlackBerry Dynamics-Profil wird verwendet, um die Sprachaufzeichnung per Tastatur zu verhindern. Es gibt jedoch bestimmte Tastaturen, die die Sprachaufzeichnung über andere Kanäle ermöglichen. (JI 2572324)

Problemumgehung: Um das Problem zu beheben, können Sie eine IT-Richtlinie anwenden, bei der die Option „Zulässige Eingabemethoden“ auf „Nur System“ gesetzt ist, oder die Installation bestimmter Tastaturen im geschäftlichen Android-Profil erzwingen.

Wenn Ihre Organisation Entrust Smart Credentials auf iOS verwendet und Sie ein Gerät deaktivieren, werden die Zertifikate auf dem Bildschirm „Profile“ weiterhin als im Import befindlich angezeigt. (JI 2569249)

Nachdem ein iOS-Benutzer ein Zertifikat importiert, wird der Benutzer erneut durch den Importprozess geführt. (JI 2538500)

* Wenn Sie einen Nur geschäftlicher Bereich-Aktivierungstyp zum Aktivieren eines Android 8.0-Geräts verwenden und ein Wi-Fi-Profil in BlackBerry UEM konfigurieren, kann der Benutzer des Geräts möglicherweise keine Verbindung zu einem Wi-Fi-Netzwerk herstellen. (JI 2371987)

Problemumgehung: Wählen Sie in der IT-Richtlinie Ihrer Organisation die Option „Änderung der Wi-Fi-Einstellung zulassen“ aus. Beachten Sie, dass dieses Problem in Android 8.1 behoben wurde.

* Wenn Sie ein Samsung Knox-Aktivierungsprofil zum Aktivieren eines Android-Geräts verwenden und die Option „Google Play App-Management für Samsung Knox Workspace-Geräte“ auswählen, wird das Gerät nicht aktiviert und es wird eine Google Play Services-Fehlermeldung angezeigt. Weitere Informationen finden Sie unter support.blackberry.com/community im Artikel KB46917. (JI 2343363)

* Auf einem Samsung Knox-Gerät werden erforderliche gehostete BlackBerry UEM-Apps möglicherweise nicht im Abschnitt „Installiert“ angezeigt, wenn der Benutzer Google Play auf dem Gerät öffnet, obwohl sie tatsächlich installiert sind. (JI 2251895)

Sie können ein macOS-Gerät nicht erneut aktivieren, wenn Sie das Aktivierungsprofil auf dem Gerät entfernen. (JI 2226652)

Bekannte Probleme mit der Verwaltungskonsole

Wenn ein BlackBerry UEM-Administrator ein Profil für Benutzeranmeldeinformationen erstellt und zuweist, das für die Verwendung einer Zertifizierungsstellenverbindung eines nativen Schlüsselspeichers konfiguriert ist, und der Benutzer eine BlackBerry Dynamics-App auf einem Android 10-Gerät öffnet, wird die folgende Fehlermeldung angezeigt: „Sie müssen ein persönliches Zertifikat auswählen. Wenn das erforderliche Zertifikat fehlt, müssen Sie es möglicherweise installieren. Versuchen Sie es erneut.“ Der Grund hierfür ist eine Änderung der KeyChain.choosePrivateKeyAlias-API in Android 10: <https://issuetracker.google.com/issues/135667502>

Für die Unterstützung nativer Schlüsselspeicher-Verbindungen in BlackBerry Dynamics-Apps auf Android 10 Geräten muss der Administrator im Profil für Benutzeranmeldeinformationen eine der folgenden Aktionen ausführen:

- Lassen Sie das Feld „Aussteller“ leer. Der Benutzer wird aufgefordert, das Zertifikat auszuwählen, wenn es erforderlich ist.
- Geben Sie einen Aussteller an, und vergewissern Sie sich, dass die Reihenfolge des relativen definierten Namens dem erforderlichen Format für Android 10 entspricht. Beispiel: „CN=core2-TKCA02-CA,DC=core2,DC=sqm,DC=testnet,DC=rims,DC=net“. Der vollständige definierte Name muss in derselben Reihenfolge wie im Zielzertifikat angegeben werden. Partielle Namen wie „DC=rims,DC=net“ sind nicht zulässig.

* Von BlackBerry Dynamics gehostete APK-Dateien werden nicht auf Geräten installiert, wenn das Aktivierungsprofil für Google Play aktiviert ist. (JI 2812745)

* In der Konsole wird keine Meldung angezeigt, wenn bei der Überprüfung der BlackBerry Dynamics-Konnektivität ein Konformitätsverstoß auftritt. (JI 2810343)

* Wenn Sie eine App-Konfiguration für eine gehostete App bearbeiten, wird möglicherweise eine doppelte App-Konfiguration erstellt. (JI 2809487)

* Benutzer von iOS-Geräten können möglicherweise nicht ohne Eingabe Ihrer Anmeldeinformationen auf Apps und Websites zugreifen, nachdem Sie ihnen ein SCEP-Profil und ein Single Sign-On-Profil zugewiesen haben. (JI 2809287)

* Die Liste der Konformitätsverstöße in der Verwaltungskonsole ist für Apps, die mit neueren SDKs erstellt wurden, möglicherweise leer. (JI 2808714)

* Eine Per App VPN-Verbindung kann nicht auf einem Gerät hergestellt werden, das mit der Aktivierungsart „Benutzerdatenschutz - Benutzerregistrierung“ aktiviert wurde. (JI 2808422)

* Die BlackBerry Connectivity-App wird möglicherweise nicht auf einem Android-Gerät bereitgestellt, das mit der Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“ (Samsung Knox) aktiviert wurde, und für das die Google Play-App-Verwaltung für Samsung Knox Workspace-Geräte aktiviert wurde. (JI 2805066)

Problemumgehung: Weisen Sie dem Gerät die APK-Datei als interne App zu, und wählen Sie die Option „App in Google-Domäne“.

* Wenn Sie auf der Registerkarte „Gerät“ versuchen, die Softwareversion auf einem überwachten iOS-Gerät auf eine bestimmte Versionsnummer zu aktualisieren und auf „Herunterladen und installieren“ klicken, wird das Betriebssystem heruntergeladen, aber nicht installiert. Ticket FB7453536 wurde für Apple erstellt. (JI 2795533)

* Wenn Sie eine interne App und ein Symbol für die App hinzufügen und auf der Seite „Apps“ auf die Schaltfläche „Aktualisieren“ klicken, wird das Symbol nicht in der App-Liste angezeigt. (JI 2790503)

* Die Sperre für Apps wird nach dem Hinzufügen einer entsprechenden Version zu *myAccount* und dem Synchronisieren der App mit BlackBerry UEM nicht aufgehoben. (JI 2777363)

* Einige Protokolldatensätze zeigen möglicherweise, dass die Weiterleitung über eine BlackBerry Proxy-Instanz erfolgte, die nicht tatsächlich verwendet wurde. (JI 2776319)

Wenn Sie die Einstellungen eines SCEP-Profiles oder Benutzeranmeldungsprofils basierend auf einem nativen Schlüsselspeicher ändern, werden die Benutzer nicht aufgefordert, die Zertifikate erneut zu registrieren, und nur neue Zertifikate erhalten die aktualisierten Einstellungen. (JI 2626894)

Problemumgehung: Löschen Sie das Profil, erstellen Sie ein neues Profil und weisen Sie es zu, um die neuen Einstellungen anzuwenden.

* Wenn Sie im BlackBerry Dynamics-Profil eine Liste mit mehr als 10000 verbotenen Kennwörtern hochladen, wird die Liste bei 10000 Kennwörtern abgeschnitten. (JI 2511201)

Wenn Sie die erweiterte Ansicht in der Verwaltungskonsole verwenden, wird auf der Seite „Gerätedetails“ ein falscher Betrag für den internen Speicher der Geräte angezeigt. (JI 2376060)

Wenn Sie eine IT-Richtlinie für Android-Geräte erstellen, impliziert die Regel „Unterschiedliches Kennwort für geschäftlichen Bereich und Gerät erzwingen“, dass die Kennwörter für den persönlichen und den geschäftlichen Bereich unterschiedlich sein müssen. Die Kennwörter können jedoch identisch sein, obwohl es separate Kennwörter sind. (JI 2206856)

Sie können die Version einer App in der BlackBerry UEM-Konsole erst dann aktualisieren, wenn die neuere Version der App in Google Play verfügbar ist. (JI 2203775)

Problemumgehung: Fügen Sie die neue Version der App Google Play hinzu, warten Sie, bis Google die App veröffentlicht hat, und fügen Sie die App dann der BlackBerry UEM-Konsole hinzu.

* Wenn Sie einen Benutzer löschen, der BlackBerry Workspaces verwenden kann, ist die angezeigte Meldung irreführend. (JI 1657607)

Problemumgehung: Melden Sie sich als BlackBerry Workspaces-Unternehmensadministrator, der über eine E-Mail-Adresse verfügt, bei der Konsole an, entfernen Sie den BlackBerry Workspaces-Dienst vom Benutzer, und löschen Sie den Benutzer.

Bekannte Probleme mit dem UEM Self-Service

Die Ablauffrist für die vom UEM Self-Service generierten Zugriffsschlüssel beträgt 24 Stunden anstelle von 30 Tagen. (JI 1659057)

Rechtliche Hinweise

©2019 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

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

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

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

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

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

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

DIE IN DIESEM DOKUMENT 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 GARANTIEEN, DIE VON BLACKBERRY FÜR TEILE VON BELIEBIGEN BLACKBERRY-PRODUKTEN ODER -DIENSTLEISTUNGEN AN ANDERER STELLE ALS IN DIESER DOKUMENTATION ANGEGEBEN WURDEN, ZU ERSETZEN.

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

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

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

Veröffentlicht in Kanada