



BlackBerry UEM

Übersicht und neue Funktionen

12.16

Inhalt

| | |
|---|-----------|
| Neuerungen in BlackBerry UEM Cloud..... | 4 |
| Neuerungen in BlackBerry UEM 12.16..... | 6 |
| Was ist BlackBerry UEM?..... | 8 |
| BlackBerry Spark Suites..... | 10 |
| Vorteile von BlackBerry Workspaces..... | 11 |
| Vorteile von BlackBerry Enterprise Identity..... | 12 |
| Vorteile von BlackBerry 2FA..... | 12 |
| Vorteile von BlackBerry UEM Notifications..... | 12 |
| Apps für Unternehmen..... | 13 |
| BlackBerry Dynamics-Apps..... | 14 |
| Unternehmens-SDKs..... | 15 |
| Wichtigste Funktionen von BlackBerry UEM..... | 18 |
| Schlüsselmerkmale aller Gerätetypen..... | 22 |
| Schlüsselmerkmale der einzelnen Gerätetypen..... | 25 |
| Kompatibilität und Anforderungen..... | 32 |
| Rechtliche Hinweise..... | 33 |

Neuerungen in BlackBerry UEM Cloud

Verwaltungskonsole

Android-App-Lizenzen: Die Android-App-Lizenzseite wurde aus der UEM-Verwaltungskonsole entfernt.

Google Play Store-Layout: Sie müssen die Funktion „Apps organisieren“ in Google Play iFrame verwenden, um Ihr Google Play Store-Layout zu verwalten. Sie können zum Verwalten des Google Play Store-Layouts nicht mehr die Dropdown-Liste „Kategorie“ in den App-Details verwenden.

VPN-Profil: Sie geben ein verknüpftes Proxy-Profil an, wenn Sie in einem VPN-Profil „IKEv2 immer aktiviert“ auswählen.

Purebred-App: Wenn Sie die neue Purebred-App Version 2.1 (8) verwenden, die über den Mechanismus zur benutzerdefinierten App-Verteilung übermittelt werden muss, müssen Sie die Uniform Type Identifiers (UTI), die Unterstriche (_) enthalten, aufgrund der BlackBerry UEM Client-App-Richtlinie zu Bindestrichen (-) aktualisieren. Verwenden Sie zum Beispiel `purebred.select.all-user; purebred.select.no-filter; purebred.zip.all-user; purebred.zip.no-filter`. Benutzer müssen die neue Purebred-App möglicherweise auf ihrem Gerät erneut aktivieren.

Kryptografische Token für iOS-Geräte: UEM unterstützt jetzt das CryptoTokenKit-Framework für iOS-Geräte, sodass BlackBerry Dynamics-Apps auf kryptografische Token von PKI-Apps zugreifen können (z. B. Purebred). Die Unterstützung für kryptografische Token ist aktiviert, wenn Sie die Verbindungsoption „Nativer Schlüsselspeicher“ und die iOS-Plattform im Profil für Benutzeranmeldeinformationen auswählen. Diese Funktion erfordert UEM 12.16 und setzt voraus, dass Apps BlackBerry Dynamics SDK 10.2 oder höher verwenden.

Profil für Benutzeranmeldeinformationen: In Profilen für Benutzeranmeldeinformationen, die als Verbindungstyp native Schlüsselspeicher verwenden, können Sie jetzt die Betriebssystem-Plattformen des Geräts angeben, auf die das Profil angewendet werden soll.

iPad

Gemeinsam genutzte iPad-Geräte: iPad-Geräte können jetzt von mehreren Benutzern gemeinsam genutzt werden. Wenn sich Benutzer mit einer Managed Apple-ID anmelden, werden ihre Daten geladen, und der Benutzer hat dann Zugriff auf seine eigenen E-Mail-Konten, Dateien, die iCloud-Fotobibliothek, App-Daten und mehr.

Android

Android-Softwareversionen: Im Profil für Gerätedienstleistungen können Sie nun Android-Betriebssystem-Updates auf Samsung-Geräte anwenden.

BlackBerry Dynamics-Profil: Im BlackBerry Dynamics-Profil wurde eine neue Einstellung hinzugefügt, mit der Sie festlegen können, ob Android-Gerätebenutzer benutzerdefinierte Tastaturen mit BlackBerry Dynamics-Apps verwenden können.

IT-Richtlinien

| Gerätetyp | Regelname | Beschreibung | Aktivierungsarten |
|-----------|-----------|--------------|-------------------|
|-----------|-----------|--------------|-------------------|

| | | | |
|---------|---|--|--|
| Android | Von VPN ausgenommene geschäftliche Anwendungen | Liste der geschäftlichen Apps, die Daten nicht über die geschäftliche Verbindung senden müssen, wenn die Option „Verwendung von VPN für geschäftliche Anwendungen erzwingen“ ausgewählt ist | <ul style="list-style-type: none"> • Nur geschäftlicher Bereich • Nur geschäftlicher Bereich (Premium) • Geschäftlich und persönlich – Benutzer-Datenschutz • Geschäftlich und persönlich – Benutzer-Datenschutz (Premium) • Geschäftlich und persönlich – vollständige Kontrolle • Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
|---------|---|--|--|

Neuerungen in BlackBerry UEM 12.16

Verwaltungskonsole

Android-App-Lizenzen: Die Android-App-Lizenzseite wurde aus der UEM-Verwaltungskonsole entfernt.

Google Play Store-Layout: Sie müssen die Funktion „Apps organisieren“ in Google Play iFrame verwenden, um Ihr Google Play Store-Layout zu verwalten. Sie können zum Verwalten des Google Play Store-Layouts nicht mehr die Dropdown-Liste „Kategorie“ in den App-Details verwenden.

VPN-Profil: Sie geben ein verknüpftes Proxy-Profil an, wenn Sie in einem VPN-Profil „IKEv2 immer aktiviert“ auswählen.

Purebred-App: Wenn Sie die neue Purebred-App Version 2.1 (8) verwenden, die über den Mechanismus zur benutzerdefinierten App-Verteilung übermittelt werden muss, müssen Sie die Uniform Type Identifiers (UTI), die Unterstriche (_) enthalten, aufgrund der BlackBerry UEM Client-App-Richtlinie zu Bindestrichen (-) aktualisieren. Verwenden Sie zum Beispiel `purebred.select.all-user; purebred.select.no-filter; purebred.zip.all-user; purebred.zip.no-filter`. Benutzer müssen die neue Purebred-App möglicherweise auf ihrem Gerät erneut aktivieren.

Kryptografische Token für iOS-Geräte: UEM unterstützt jetzt das CryptoTokenKit-Framework für iOS-Geräte, sodass BlackBerry Dynamics-Apps auf kryptografische Token von PKI-Apps zugreifen können (z. B. Purebred). Die Unterstützung für kryptografische Token ist aktiviert, wenn Sie die Verbindungsoption „Nativer Schlüsselspeicher“ und die iOS-Plattform im Profil für Benutzeranmeldeinformationen auswählen. Diese Funktion erfordert UEM 12.16 und setzt voraus, dass Apps BlackBerry Dynamics SDK 10.2 oder höher verwenden.

Profil für Benutzeranmeldeinformationen: In Profilen für Benutzeranmeldeinformationen, die als Verbindungstyp native Schlüsselspeicher verwenden, können Sie jetzt die Betriebssystem-Plattformen des Geräts angeben, auf die das Profil angewendet werden soll.

iPad

Gemeinsam genutzte iPad-Geräte: iPad-Geräte können jetzt von mehreren Benutzern gemeinsam genutzt werden. Wenn sich Benutzer mit einer Managed Apple-ID anmelden, werden ihre Daten geladen, und der Benutzer hat dann Zugriff auf seine eigenen E-Mail-Konten, Dateien, die iCloud-Fotobibliothek, App-Daten und mehr.

Android

Android-Softwareversionen: Im Profil für Gerätedienstleistungen können Sie nun Android-Betriebssystem-Updates auf Samsung-Geräte anwenden.

BlackBerry Dynamics-Profil: Im BlackBerry Dynamics-Profil wurde eine neue Einstellung hinzugefügt, mit der Sie festlegen können, ob Android-Gerätebenutzer benutzerdefinierte Tastaturen mit BlackBerry Dynamics-Apps verwenden können.

IT-Richtlinien

| Gerätetyp | Regelname | Beschreibung | Aktivierungsarten |
|-----------|-----------|--------------|-------------------|
|-----------|-----------|--------------|-------------------|

| | | | |
|---------|---|--|--|
| Android | Von VPN ausgenommene geschäftliche Anwendungen | Liste der geschäftlichen Apps, die Daten nicht über die geschäftliche Verbindung senden müssen, wenn die Option „Verwendung von VPN für geschäftliche Anwendungen erzwingen“ ausgewählt ist | <ul style="list-style-type: none"> • Nur geschäftlicher Bereich • Nur geschäftlicher Bereich (Premium) • Geschäftlich und persönlich – Benutzer-Datenschutz • Geschäftlich und persönlich – Benutzer-Datenschutz (Premium) • Geschäftlich und persönlich – vollständige Kontrolle • Geschäftlich und persönlich – vollständige Kontrolle (Premium) |
|---------|---|--|--|

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- und Windows 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. BlackBerry UEM Cloud senkt die Betriebskosten, da keine Services installiert, verwaltet und aktualisiert werden müssen. |
| Eine einzige webbasierte Schnittstelle | Verwaltung von iOS-, macOS-, Android- und Windows 10-Geräten und weiteren 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 UEMNotifications (nur BlackBerry UEM lokal), mit denen Sie den Wert Ihrer BlackBerry UEM-Bereitstellung steigern können. |

Weitere Informationen zu BlackBerry UEM finden Sie in der [Dokumentation für Administratoren](#).

BlackBerry Spark Suites

Neben den Sicherheits- und Produktivitätsfunktionen, die BlackBerry UEM bietet, vereinheitlichen BlackBerry Spark Suites Lösungen für Endpunktverwaltung und -sicherheit, um die Anforderungen von Unternehmen und Organisationen zu erfüllen.

Sicherheitsbewusste Unternehmen wechseln zu einem Zero-Trust-Ansatz, um die Netzwerksicherheit zu modernisieren und gleichzeitig das Netzwerkerlebnis für Endbenutzer zu verbessern. Das Zero-Trust-Sicherheitsmodell vertraut standardmäßig nichts und niemandem, einschließlich Benutzern im geschäftlichen Netzwerk. Jeder Benutzer, jeder Endpunkt und jedes Netzwerk wird als potenziell gefährlich angesehen. Bei Zero-Trust-Sicherheit kann ein Benutzer erst auf alles zugreifen, wenn er nachgewiesen hat, wer er ist, dass sein Zugriff autorisiert ist, dass das Netzwerk, mit dem er verbunden ist, nicht gefährdet ist und dass er oder sich auf seinem Gerät befindliche Malware nicht böswillig handelt.

Weitere Informationen zu BlackBerry Spark Suites und darin enthaltenen Produkten finden Sie in [der Übersicht zu BlackBerry Spark](#).

| Suite | Beschreibung |
|------------------------|--|
| BlackBerry Spark Suite | <p>BlackBerry Spark Suite ist der Goldstandard für einheitliche Endpunktsicherheit und -verwaltung. Es umfasst BlackBerry Spark UEM Suite und die BlackBerry Cyber Suite in einem Paket, das umfassende Funktionen für Endpunktverwaltung und -sicherheit bietet, um Ihr Unternehmen vor mehreren Bedrohungen zu schützen.</p> <p>BlackBerry Spark Suite kombiniert das von BlackBerry Cyber Suite angebotene Zero-Trust-Modell für Unified Endpoint Security und die bewährte BlackBerry Spark UEM Suite für Endpunktverwaltung, um eine vollständige Palette an BlackBerry-Unternehmensprodukten für die Verwaltung und Sicherung all Ihrer Endpunkte und die Kommunikation zwischen ihnen bereitzustellen. Mit dieser Suite erhalten Sie alle Produkte im Cyber Suite und Spark UEM Suite sowie die Möglichkeit, CylancePROTECT Mobile über die Verwaltungskonsole der jeweiligen Suite zu verwalten.</p> |
| BlackBerry Cyber Suite | <p>BlackBerry Cyber Suite bietet eine einheitliche Endpunktsicherheit für Ihr Unternehmen, um bössartige Angriffe mithilfe von KI-gestützten Informationen und Reaktionsmechanismen zu überwachen und zu verhindern. BlackBerry Cyber Suite arbeitet mit allen MDM-Anbietern zusammen, um Ihre Sicherheitsanforderungen zu erfüllen, auch wenn Ihre Geräteverwaltungsanforderungen nicht die Raffinesse von BlackBerry UEM erfordern.</p> <p>BlackBerry Cyber Suite bietet folgende Vorteile:</p> <ul style="list-style-type: none">• Bietet einen Pfad von der Zero-Trust-Architektur zur Zero-Touch-Erfahrung mit starker KI• Funktioniert mit jeder Plattform für Unified Endpoint Management (UEM) oder Mobile Device Management (MDM)• Bietet kontinuierliche Überwachung und Bedrohungserkennung• Bietet kontextbezogene und kontinuierliche Authentifizierung, die Endpunkte, Netzwerke, Apps und Personen umfasst |

| Suite | Beschreibung |
|------------------------------------|---|
| BlackBerry Spark UEM Suite | <p>BlackBerry Spark UEM Suite bietet eine erstklassige einheitliches Endpunktverwaltung. Es bietet den vollen Funktionsumfang von BlackBerry UEM, dem Behörden, Unternehmen und andere Organisationen seit langem vertrauen, um die Kommunikation mit mobilen Geräten zu verwalten und zu sichern, sowie Identitätsmanagement, Zwei-Faktor-Authentifizierung und digitale Rechteverwaltung zu nutzen, damit Benutzer sicher auf geschäftliche Ressourcen zugreifen und von überall aus arbeiten können.</p> <p>BlackBerry Spark UEM Suite fügt die folgenden Produkte zu BlackBerry UEM hinzu:</p> <ul style="list-style-type: none"> • BlackBerry Enterprise Identity • BlackBerry 2FA • BlackBerry Workspaces • BlackBerry Dynamics-Apps • BlackBerry Dynamics SDK <p>Weitere Informationen zu allen Produkten in der Suite und wie sie zusammenarbeiten, finden Sie in der Übersicht zu BlackBerry Spark.</p> |
| BlackBerry Spark UEM Express Suite | <p>BlackBerry Spark UEM Express Suite ist eine ideale Lösung für Geräteverwaltung und Produktivität für kleinere Unternehmen und Organisationen. Es umfasst die wichtigsten Funktionen zur Verwaltung der Geräte von Benutzern, unabhängig davon, ob die Geräte von Ihrem Unternehmen bereitgestellt werden oder im Besitz Ihrer Mitarbeiter sind, und schützt gleichzeitig Ihre Daten. Sie können Benutzer mit geschäftlichen Apps ausstatten, die sichere geschäftliche E-Mails, sicheres Surfen im Internet und den Intranet-Zugriff, Aufgabenverwaltung und Instant Messaging ermöglichen, um produktiv zu sein.</p> <p>BlackBerry Spark UEM Express Suite umfasst BlackBerry UEM und die beliebtesten BlackBerry Dynamics-Apps, um gängige Geschäftsanforderungen zu erfüllen.</p> |

Eine visuelle Übersicht über die BlackBerry Spark Suiten [finden Sie in der visuellen Einführung](#).

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 an 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- und Android-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-Verwaltungskonsolle 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](#).

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 und Android 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 Kontrolle aller Ihrer 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.

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- und Android-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) 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.

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-Verwaltungskonsole 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 ist nur für die Verwendung von lokalen BlackBerry UEM-Systemen verfügbar.

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 | <p>Der 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 aus App Store und für Android-Geräte von Google Play herunterladen. Nachdem Benutzer ihre Geräte aktiviert haben, bietet der BlackBerry UEM Client folgende Möglichkeiten:</p> <ul style="list-style-type: none"> • Überprüfung der Konformität ihrer Geräte mit den Standards des Unternehmens • Ansicht der Profile, die ihren Benutzerkonten zugewiesen sind • Ansicht der IT-Richtlinienregeln, die ihren Benutzerkonten zugewiesen sind • Zugriff auf geschäftliche Apps • Erstellen von Zugriffsschlüsseln für BlackBerry Dynamics-Apps • Vorauthentifizierung mit BlackBerry 2FA • Zugriff auf einen Software-OTP-Code • Abrufen und Versenden von Geräteprotokolldateien per E-Mail • Deaktivieren ihrer Geräte <p>Weitere Informationen finden Sie in der Dokumentation zu BlackBerry UEM Client.</p> |
| BlackBerry Dynamics-Apps | <p>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.</p> |

| Komponente | Beschreibung |
|----------------|--|
| BBM Enterprise | <p>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-, Windows- und macOS-Geräte verfügbar.</p> <p>BBM Enterprise verwendet eine gemäß FIPS 140-2 validierte kryptographische Bibliothek. Die Verschlüsselungsschlüssel gehören Ihrem Unternehmen und sonst niemandem. Nicht einmal BlackBerry kann darauf zugreifen.</p> <p>Bei den meisten Geräten können Sie BBM Enterprise Benutzern mithilfe von BlackBerry UEM 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.</p> <p>BBM Enterprise ist separat erhältlich in den BlackBerry Spark Suites.</p> |

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 | <p>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.</p> <p>Weitere Informationen zu BlackBerry Work inden Sie in der Dokumentation zu BlackBerry Work.</p> |
| BlackBerry Access | <p>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.</p> <p>Weitere Informationen zu BlackBerry Access inden Sie in der Dokumentation zu BlackBerry Access.</p> |
| BlackBerry Connect | <p>BlackBerry Connect unterstützt Kommunikation und Zusammenarbeit mit sicherem Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen über eine benutzerfreundliche Schnittstelle auf dem Gerät des Benutzers.</p> <p>Weitere Informationen zu BlackBerry Connect inden Sie in der Dokumentation zu BlackBerry Connect.</p> |

| App | Beschreibung |
|------------------------------|--|
| BlackBerry Tasks | BlackBerry Tasks ermöglicht Benutzern das Erstellen, Bearbeiten und Verwalten von Aufgaben und deren Synchronisierung mit Microsoft Exchange. Weitere Informationen zu BlackBerry Tasks inden Sie in der Dokumentation zu BlackBerry Tasks. |
| BlackBerry Notes | BlackBerry Notes ermöglicht Benutzern, Notizen, die mit Microsoft Exchange auf einem beliebigen Mobilgerät synchronisiert wurden, zu erstellen, zu bearbeiten und zu verwalten. Weitere Informationen zu BlackBerry Notes inden Sie in der Dokumentation zu BlackBerry Notes. |
| 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. Weitere Informationen zu BlackBerry Enterprise BRIDGE inden Sie in der Dokumentation zu BlackBerry Enterprise BRIDGE. |

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

Sie können auch eigene BlackBerry Dynamics-Apps mithilfe des BlackBerry Dynamics-SDK 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. Weitere Informationen zu BlackBerry UEM Integration SDK finden Sie in der Dokumentation BlackBerry UEM Integration SDK . |

| Komponente | Beschreibung |
|-----------------------------------|---|
| BlackBerry Dynamics SDK | <p>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:</p> <ul style="list-style-type: none"> • Sicherheitsdienste (z. B. sichere Kommunikation und APIs für den Datenaustausch zwischen Apps) • Mobile Dienste (z. B. Anwesenheit, E-Mail, Push, Directory Lookup) • Plattformservices (z. B. Authentifizierung per einmaliger Anmeldung, Identitäts- und Zugriffsmanagement, App-Steuer-elemente für Administratoren) <p>Weitere Informationen zu BlackBerry Dynamics SDK finden Sie in der Dokumentation BlackBerry Dynamics SDK.</p> |
| BlackBerry Analytics SDK | <p>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.</p> <p>Weitere Informationen zu BlackBerry Analytics SDK finden Sie in der Dokumentation BlackBerry Analytics.</p> |
| Spark Communications Services-SDK | <p>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.</p> <p>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.</p> <p>Weitere Informationen zum Spark Communications Services finden Sie in der Dokumentation zum Spark Communications Services-SDK.</p> |
| BlackBerry Web Services | <p>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.</p> <p>Weitere Informationen zu BlackBerry Web Services finden Sie in der Dokumentation zu BlackBerry Web Services für BlackBerry UEM.</p> |

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 und Windows 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 Verwaltungskonsolle 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 zu 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 iOS-, Samsung Knox Workspace- und Android-Geräten mit geschäftlichem Profil 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 | <p>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 mit mehreren Verzeichnissen. Sie können eine beliebige Kombination von Microsoft Active Directory und LDAP verwenden.</p> <p>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.</p> <p>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.</p> <p>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.</p> |
| 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 Vorlauf- und Wartungskosten selbst warten müssen. |

| Funktion | Beschreibung |
|--------------------------|---|
| Migration | <p>Sie können Benutzer, Geräte, Gruppen und andere Daten von einer lokalen BlackBerry UEM-Quelldatenbank auf eine neue lokale oder BlackBerry UEM Cloud-Instanz migrieren.</p> <p>Wenn Sie BlackBerry UEM für die Verwaltung von Google Play-Konten konfiguriert haben, können Sie Android Enterprise-Geräte von einem lokalen BlackBerry UEM-Server auf BlackBerry UEM Cloud oder einen anderen lokalen BlackBerry UEM-Server migrieren.</p> <p>Sie können BlackBerry Dynamics-Benutzer von der lokalen BlackBerry UEM (Version 12.13 oder höher) zu einem BlackBerry UEM Cloud migrieren.</p> |
| Cisco ISE-Integration | <p>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.</p> |
| Regionale Bereitstellung | <p>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 mit Zuordnung zu diesen Profilen 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.</p> |
| Wearable-Geräte | <p>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-Profilen, App-Management und standortbezogene Dienste.</p> |

| Funktion | Beschreibung |
|------------------------------|---|
| Microsoft Intune-Integration | <p>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 während der Verwendung von BlackBerry UEM zur Geräteverwaltung 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.</p> |

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 | <p>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.</p> <p>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.</p> |
| Geräte verwalten | <p>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 Gerätebestand Ihres Unternehmens anzeigen. Sie können die folgenden Aktionen durchführen, sofern diese vom Gerät unterstützt werden:</p> <ul style="list-style-type: none"> • Sperren des Geräts, Ändern des Kennworts für das Gerät bzw. für den geschäftlichen Bereich oder Löschen der Informationen vom Gerät • Sicheres Verbinden des Geräts mit der E-Mail-Umgebung Ihres Unternehmens durch Verwendung von Microsoft Exchange ActiveSync zur Unterstützung von E-Mail und Kalender • Steuern, wie das Gerät auf das Unternehmensnetzwerk, einschließlich Wi-Fi und VPN-Einstellungen, zugreifen kann • Konfigurieren der einmaligen Anmeldung für das Gerät, sodass es sich automatisch bei Domänen und Webdiensten innerhalb Ihres Unternehmensnetzwerks authentifiziert • Steuern der Funktionen des Geräts, u. a. Einrichten von Regeln für die Kennwortsicherheit und Deaktivieren von Funktionen, z. B. die Kamera • Verwalten der App-Verfügbarkeit auf dem Gerät, einschließlich der Angabe von App-Versionen und ob die Apps obligatorisch oder optional sind • Durchsuchen von App Stores direkt nach Apps, die Geräten zugewiesen werden können • Installieren von Zertifikaten auf dem Gerät und optionales Konfigurieren von SCEP, um die automatische Zertifikatsanmeldung zuzulassen • Erweitern der E-Mail-Sicherheit mithilfe von S/MIME oder PGP |
| Verwalten von Benutzergruppen, Apps und Geräten | <p>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.</p> |

| 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-Profiles 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 | <p>Auf allen verwalteten Geräten sind geschäftliche Apps solche, die den Benutzern von Unternehmen zur Verfügung gestellt werden. Beachten Sie, dass UEM die App-Verwaltung für macOS nicht unterstützt. Weitere Informationen zur Aktivierung der MDM-Steuererelemente für macOS finden Sie in den Informationen zum Aktivieren von Geräten.</p> <p>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.</p> |
| 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 |
|--|--|
| <p>Hohe Verfügbarkeit und Notfallwiederherstellung für die BlackBerry Infrastructure und BlackBerry UEM Cloud Umgebungen</p> | <p>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 Zugang zu Gebäuden, Überwachungsfunktionen und Hardwareredundanzen, um die Daten Ihres Unternehmens vor Naturkatastrophen und nicht autorisiertem Zugriff zu schützen.</p> <p>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.</p> |
| <p>Zertifikatsbasierte Authentifizierung</p> | <p>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.</p> |
| <p>Verwalten von Lizenzen für bestimmte Funktionen und Gerätesteuern</p> | <p>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.</p> |

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 | <p>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.</p> <p>Sie können mehrere Apple-DEP-Konten mit einer BlackBerry UEM-Domäne verknüpfen.</p> |
| 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 benutzerdefinierter Payload-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 | <p>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.</p> |
| Integration mit BlackBerry Dynamics | <p>Sie können das BlackBerry Dynamics-Profil verwenden, um iOS-Geräten den Zugriff auf BlackBerry Dynamics-Produktivitäts-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.</p> <p>Das Profil ermöglicht die Aktivierung von BlackBerry Dynamics für Benutzer, die bereits für BlackBerry Dynamics aktiviert sind.</p> |
| Per-App-VPN | <p>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.</p> <p>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.</p> |
| Apple-Aktivierungssperre | <p>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.</p> |
| Persönliche App-Listen | <p>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 Verwaltungskonsolle eine Liste aller persönlichen Apps anzeigen, die in persönlichen Bereichen der Benutzer installiert sind.</p> |
| Verloren-Modus für überwachte iOS-Geräte | <p>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.</p> |
| IBM Notes Traveler-Unterstützung | <p>iOS-Geräte können eine Verbindung zu IBM Notes Traveler über den BlackBerry Secure Gateway herstellen.</p> |

| 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 | <p>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 Anmeldeprozesses von BlackBerry UEM verwaltet. Diese Funktion wurde speziell für überwachte Geräte mit der folgenden Konfiguration entwickelt:</p> <ul style="list-style-type: none"> • App-Sperrmodus aktiviert • VPP-Apps zugewiesen |
| iPad | iPad-Geräte können von mehreren Benutzern gemeinsam genutzt werden. Wenn sich Benutzer mit einer Managed Apple-ID anmelden, werden ihre Daten geladen, und der Benutzer hat dann Zugriff auf seine eigenen E-Mail-Konten, Dateien, die iCloud-Fotobibliothek, App-Daten und mehr. |

Android-Geräte

| Funktion | Beschreibung |
|---|--|
| Android Enterprise-Geräte verwalten | <p>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.</p> <p>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 Löschrrechte vorbehalten.</p> <p>Samsung und BlackBerry auf Android-Geräten bieten zusätzliche Administratoroptionen, unter anderem auch (bei einer Aktivierung mit Android Enterprise) erweiterte IT-Richtlinienregeln.</p> <p>Kunden, die BlackBerry UEM für die Verwaltung von Google Play-Konten konfiguriert haben, können nun Android Enterprise-Geräte von einem lokalen BlackBerry UEM-Server in die UEM Cloud oder einen anderen lokalen BlackBerry UEM-Server migrieren.</p> |
| 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 | <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Erweiterte IT-Richtlinienregeln • Erweiterte Anwendungsverwaltung, einschließlich automatischer Installation und Deinstallation von Apps, automatischer Deinstallation gesperrter Apps und Verhinderung der Installation gesperrter Apps • App-Sperrmodus <p>Weitere Informationen zu den unterstützten Geräten finden Sie in der Kompatibilitätsmatrix. Weitere Informationen zu Knox finden Sie unter https://www.samsungknox.com.</p> |
| Integration mit BlackBerry Dynamics | <p>Sie können das BlackBerry Dynamics-Profil verwenden, um Android-Geräten den Zugriff auf BlackBerry Dynamics-Produktivitäts-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.</p> <p>Das Profil ermöglicht die Aktivierung von BlackBerry Dynamics für Benutzer, die bereits für BlackBerry Dynamics aktiviert sind.</p> |
| Per-App-VPN | <p>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.</p> |
| Zero-Touch-Registrierung | <p>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.</p> |

| 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 Smart Credentials zur Signatur, Verschlüsselung und Authentifizierung für BlackBerry Dynamics-Apps und Apps im geschäftlichen Bereich von Android Enterprise- und Samsung Knox Workspace-Geräten. |
| Schutz für Android Enterprise-Geräte beim Zurücksetzen auf die Werkseinstellungen | Sie können für die Android Enterprise-Geräte Ihres Unternehmens, bei denen nur der geschäftliche Bereich aktiviert ist, ein Schutzprofil für den Fall anlegen, dass sie auf die Werkseinstellungen zurückgesetzt werden. 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-Profiles Windows 10 Mobile für Geräte einrichten. |

| Funktion | Beschreibung |
|---|--|
| Per-App-VPN | <p>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.</p> <p>Für Windows 10-Geräte werden im VPN-Profil Apps der App-Auslöserliste hinzugefügt.</p> |
| Windows-Datenschutz für Windows 10-Geräte | <p>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.</p> |
| Whitelist für Virenschutzanbieter | <p>Im Konformitätsprofil können Sie unter der Regel „Antivirus-Status“ für Windows-Geräte festlegen, Antivirensoftware von beliebigen Herstellern zuzulassen, 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.</p> |
| Azure Active Directory-Einbindung | <p>BlackBerry UEM unterstützt die Azure Active Directory-Einbindung, um den MDM-Registrierungsvorgang für Windows 10-Geräte zu vereinfachen. Benutzer können Ihre Geräte bei BlackBerry UEM unter Zuhilfenahme ihres Azure Active Directory-Benutzernamens und -Kennworts registrieren. Die Azure Active Directory-Einbindung unterstützt außerdem Windows AutoPilot, sodass Windows 10-Geräte während der vorkonfigurierten Windows 10-Einrichtung automatisch mit BlackBerry UEM aktiviert werden können. Hinweis: Um die automatische MDM-Registrierung mit BlackBerry UEM während der Windows 10-Out-of-the-Box-Einrichtung zu aktivieren, muss auf dem Gerät ein BlackBerry UEM-Zertifikat installiert sein.</p> |

macOS-Geräte

| Funktion | Beschreibung |
|--|--|
| Grundlegende Geräteverwaltung mithilfe von Gerätesteuerungen | <p>Wenn ein Benutzer ein macOS-Gerät aktiviert, werden das Gerät und der Benutzer als separate Einheiten auf BlackBerry UEM eingerichtet. Zwischen BlackBerry UEM und dem Gerät und BlackBerry UEM und dem Benutzerkonto werden separate Kommunikationskanäle eingerichtet, sodass Sie das Gerät und den Benutzer getrennt verwalten können.</p> |

| Funktion | Beschreibung |
|-------------------------|---|
| Profile und Richtlinien | <p data-bbox="496 268 1435 394">Einige Profile werden nur dem Benutzer zugewiesen, z. B. E-Mail-Profile. Einige Profile werden nur dem Gerät zugewiesen, z. B. Proxy-Profile. Bei manchen Profilen können Sie wählen, ob das Profil für das Gerät oder den Benutzer gelten soll (zum Beispiel Wi-Fi-Profile).</p> <p data-bbox="496 415 1425 474">Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern. Benutzer aktivieren macOS-Geräte mithilfe von BlackBerry UEM Self-Service.</p> |

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

©2022 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

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, ZUFRIEDENSTELLENDE 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 MANGELNDE 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 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, VERSCHÄRFTE SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIRECTE, KONKRETE,

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada