BlackBerry UEM

Übersicht und neue Funktionen

12.9

Inhalt

Neuerungen in BlackBerry UEM 12.9

Unterstützung der von Entrust IdentityGuard abgeleiteten Anmeldeinformationen

Abgeleitete Anmeldeinformationen: Verwenden Sie von Entrust IdentityGuard abgeleitete intelligente Anmeldeinformationen zur Signatur, Verschlüsselung und Authentifizierung für BlackBerry Dynamics-Apps und Apps im geschäftlichen Bereich im Android-Arbeitsprofil und auf Samsung KNOX Workspace-Geräten. (JI 2221272)

Android

Security Patch-Einstellungen können Geräten aller Hersteller sowie allen Modellen in Konformitätsprofilen für Android-Geräte zugewiesen werden: Wenn Sie ein Konformitätsprofil für Android-Geräte konfigurieren und die Option „Erforderliche Security Patch-Stufe fehlt“ auswählen, können Sie jetzt die Option „Alle Anbieter > Alle Modelle“ in der Liste der zugelassenen Gerätemodelle auswählen. Dadurch können Sie ein Sicherheitspatch auf jedes Gerät anwenden, das Android OS verwendet. (JI 2241159)

Die Security Patch-Version kann auf einen Tag im Monat in Konformitätsprofilen für Android-Geräte festgelegt werden: Wenn Sie ein Konformitätsprofil für Android-Geräte konfigurieren und die Option „Erforderliche Security Patch-Stufe fehlt“ auswählen, können Sie jetzt die Patch-Stufe basierend auf dem Tag zusätzlich zum Monat und Jahr festlegen. (JI 2241159)

Android Gerätekennwort zurücksetzen: Der Administrator kann den Befehl **Gerätekennwort festlegen und sperren** für aktivierte Geräte verwenden, die die (Premium)-Aktivierungsarten Geschäftlich und persönlich – Benutzer-Datenschutz und Geschäftlich und persönlich – Benutzer-Datenschutz verwenden. Mit diesem Befehl können Sie ein Gerätekennwort erstellen und das Gerät anschließend sperren. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Um das Gerät zu entsperren, muss der Benutzer das neue Kennwort eingeben. Nur BlackBerry-Geräte mit Android 8.x und höher unterstützen diesen Befehl. (JI 2249999)

Registrieren: BlackBerry UEM unterstützt jetzt das Hinzufügen von Server- und Benutzernameninformationen für die Android-Zero-Touch-Registrierung, wodurch die Endbenutzeraktivierung vereinfacht wird. (JI 1674464)

Entfernen von Daten auf SD-Karten beim Löschen von Geräten, die nur für den geschäftlichen Bereich verwendet werden: Sie haben die Möglichkeit, alle Daten auf der SD-Karte in einem Gerät zu löschen, wenn Sie alle Arbeitsdaten von einem Android-Gerät mit einer Aktivierung, die nur für den geschäftlichen Bereich verwendet wird, löschen. (JI 1352406)

Steuern von Android-OS-Updates auf Android-Geräten mit Arbeitsprofil mit einer Aktivierung, die nur für den geschäftlichen Bereich verwendet wird: Sie können festlegen, wann Android-Systemaktualisierungen auf Android-Geräten mit Arbeitsprofil, die nur für den geschäftlichen Bereich verwendet werden, angewendet werden sollen. Verwenden Sie das Device-SR-Profil, um Regeln nach Android-Gerätemodell und -Betriebssystemversion festzulegen. (JI 1352406)

iOS

Funktion zur Einschränkung der Verwaltung auf iOS-Geräten: Administratoren können jetzt die Anzahl MDM-basierter Steuerelemente auf iOS-Geräten einschränken und die Privatsphäre des Benutzers für MDM-Anmeldungen mit selektiven MDM-Steuerelementen in den Benutzerdatenschutzaktivierungen verbessern. Mit den neuen Steuerungen können Administratoren nur die Geräteteile steuern, die für das Unternehmen wichtig sind. Gleichzeitig wird die Privatsphäre der Benutzer und der Nutzung persönlicher Apps gewahrt. (JI 1538477)

Funktion zur einfachen Ablehnung neuer Apps für iOS-Geräte: Nutzer von iOS-Geräten können neue Apps, die in der Registerkarte „Neu“ des App-Katalogs geschäftlicher Apps aufgeführt sind, jetzt bestätigen und ablehnen,

indem sie zwischen den Registerkarten wechseln. Installierte Apps, für die ein Update bereitsteht, bleiben in der Liste enthalten. Auch die Ladezeit des App-Katalogs wurde verbessert. (JI 2354245)

iOS 11.3 Web Clip-Symbole: Sie können jetzt Web Clip-Symbole zum Layoutprofil für den Startbildschirm hinzufügen. (JI 2502748)

iOS 11.3 Richtlinienaktualisierungen: Die folgenden neuen Richtlinien sind für iOS-Geräte (JI 2502748) mit der Version 11.3 verfügbar:

- Verzögerte Software-Updates anzeigen (nur unter Aufsicht)
- USB-Verbindungen zulassen, wenn Gerät gesperrt ist (nur unter Aufsicht)
- Vor dem automatischen Ausfüllen sensibler Daten Authentifizierung anfordern (nur unter Aufsicht)
- Automatische Einrichtung neuer Geräte zulassen (nur unter Aufsicht)
- Softwareupdates verzögern (nur unter Aufsicht)

Verwaltungskonsole

Apps einen Rang zuweisen: Sie können iOS- und Android-Apps einen Rang zuweisen, um die Reihenfolge zu steuern, in der sie installiert werden, wenn Sie sie Geräten zuweisen. (JI 2483990)

Ereignisbenachrichtigungen: Administratoren können festlegen, bei folgenden Ereignissen (JI 2191964) per E-Mail informiert zu werden:

- Lizenzen laufen demnächst ab
- Die Verbindung zum Apple-DEP-Server wurde hergestellt
- Die Verbindung zum Apple-DEP-Server wurde getrennt
- Die Verbindung zum Microsoft Active Directory- oder LDAP-Server wurde getrennt

Neue Sicherheitsprofileinstellungen der Microsoft Intune-App: Das Sicherheitsprofil der Microsoft Intune-App enthält neue Einstellungen, die von Microsoft zu Intune hinzugefügt wurden. Diese ermöglichen das Deaktivieren von App-PINs, wenn für das Gerät ein Kennwortschutz erforderlich ist, und das Erfordern von Mindest-Android-Patch-Versionen. (JI 2373165)

Benutzer-Benachrichtigen aktivieren, wenn ein Gerät aktiviert wurde: Sie können BlackBerry UEM aktivieren, um einen Benutzer immer zu benachrichtigen, wenn ein Gerät auf seinem Konto aktiviert wurde. Die E-Mail-Benachrichtigung wird an die E-Mail-Adresse des Benutzerkontos gesendet, mit dem das Gerät aktiviert wurde. Die E-Mail enthält standardmäßig das Gerätemodell, die Seriennummer und IMEI. Wenn der Benutzer eine Benachrichtigung erhält, die er nicht erwartet hat, sollte er einen Administrator kontaktieren. (JI 2212924)

Letzte Kontaktzeit: Für Geräte, die BlackBerry Dynamics-Apps verwenden, wurde auf der Seite mit den Gerätedetails die Spalte „Letzte Kontaktzeit“ in der BlackBerry Dynamics-Apps-Liste hinzugefügt. Die Einträge in der Spalte zeigen an, wann die Apps zuletzt BlackBerry UEM kontaktiert haben. (JI 1684311)

BlackBerry Dynamics

Symbolindikator/Kennzeichen: BlackBerry Dynamics-Benutzern wird jetzt ein Symbolindikator/Kennzeichen auf dem App-Symbol im Launcher angezeigt, wenn neue Apps zugewiesen oder vorhandene benutzerdefinierte Apps aktualisiert werden. (JI 2192742)

Installation und Migration

Datenbankkonsolidierung: Während eines Upgrades auf BlackBerry UEM-Version 12.9 ab BlackBerry UEM-Version 12.7 oder höher wird der BlackBerry UEM-Installer 12.9 die vorhandenen Datenbanken BlackBerry Control und BlackBerry UEM zu einer einzigen BlackBerry UEM-Datenbank konsolidieren. (JI 2369045)

Dienstkonsolidierung: Während eines Upgrades auf BlackBerry UEM-Version 12.9 ab BlackBerry UEM-Version 12.7 oder höher wird der BlackBerry Control-Dienst entfernt und mit der BlackBerry UEM Core Komponente konsolidiert. (JI 2369045).

Verbesserte Benutzererfahrung während eines Upgrades

BlackBerry Dynamics: Die Verbindung bleibt für BlackBerry Dynamics-Benutzer aktiviert, während für die Server BlackBerry UEM und BlackBerry Connectivity Node ein Upgrade durchgeführt wird. Diese Funktion wird nur unterstützt, wenn Sie vor dem Upgrade auf BlackBerry UEM 12.9. bereits BlackBerry UEM 12.8.1 oder höher verwenden. (JI 2219869)

BlackBerry Secure Connect Plus: Die Verbindung bleibt für Benutzer von BlackBerry Secure Connect Plus-Geräten aktiviert, während für die Server BlackBerry UEM und BlackBerry Connectivity Node ein Upgrade durchgeführt wird. Diese Funktion wird nur unterstützt, wenn Sie vor dem Upgrade auf BlackBerry UEM 12.9. bereits BlackBerry UEM 12.8.1 oder höher verwenden. (JI 1685860)

UEM Notifications

UEM Notifications auf eine bestimmte Berechtigung in BlackBerry UEM beschränken: Administratoren müssen über die Berechtigung „E-Mail an mehrere Benutzer senden“ in BlackBerry UEM verfügen, um auf UEM Notifications zugreifen zu können.

REST-API

Einzelheiten zu den neuen Ergänzungen und Änderungen für die BlackBerry UEM-REST-APIs finden Sie in *BlackBerry UEM REST-API-Referenz Version 12.9* hier.

Neue IT-Richtlinienregeln

Gerätetyp	Gruppe	Name	Beschreibung
Geschäftliche Android-Profile	Gerätefunktionalität	Bluetooth-SPP zulassen	Legen Sie fest, ob die Verwendung von Bluetooth-SPP auf dem Gerät zulässig ist.
Geschäftliche Android-Profile	Gerätefunktionalität	Bluetooth PBAP zulassen	Legen Sie fest, ob ein Gerät Kontakte mit anderen Bluetooth-fähigen Geräten über Bluetooth PBAP austauschen darf.
Geschäftliche Android-Profile	Gerätefunktionalität	Bluetooth HSP zulassen	Legen Sie fest, ob die Verwendung von Bluetooth HSP auf dem Gerät zulässig ist. Über Bluetooth HSP kann sich ein Bluetooth-Headset mit dem Gerät verbinden.

Gerätetyp	Gruppe	Name	Beschreibung
Geschäftliche Android-Profile	Gerätefunktionalitä	Bluetooth HFP zulassen	Legen Sie fest, ob die Verwendung von Bluetooth HFP auf dem Gerät zulässig ist. Über Bluetooth HFP kann ein Gerät einem Bluetooth-fähigen Gerät (z. B. einer Freisprechanlage oder einem Headset) ermöglichen, auf die Kontakte und Telefon-Apps des Geräts zuzugreifen, um Anrufe zu tätigen.
Geschäftliche Android-Profile	Gerätefunktionalität	Bluetooth AVRCP zulassen	Legen Sie fest, ob die Verwendung von Bluetooth AVRCP auf dem Gerät zulässig ist. Über Bluetooth AVRCP kann ein Gerät einem Bluetooth-fähigen Geräte (z. B. einem Headset) erlauben, Medien-Apps auf dem Gerät zu steuern.
Geschäftliche Android-Profile	Gerätefunktionalitä	Bluetooth A2DP zulassen	Legen Sie fest, ob die Verwendung von Bluetooth A2DP auf dem Gerät zulässig ist. Ein Gerät kann Bluetooth A2DP verwenden, um Audiodateien auf ein anderes Bluetooth-fähiges Gerät (z. B. ein Headset) zu streamen.
Geschäftliche Android-Profile	Gerätefunktionalität	VPN-Verbindung dauerhaft erzwingen	Legen Sie fest, ob eine VPN-Verbindung für geschäftliche Daten immer verfügbar ist. Weitere Informationen dazu finden Sie unter http://support.blackberry.com/kb im Artikel KB48330.
Geschäftliche Android-Profile	Gerätefunktionalitä	Verwendung von BlackBerry Secure Connect Plus für eine VPN-Verbindung	Legen Sie fest, ob BlackBerry Secure Connect Plus die VPN-Verbindung bereitstellt, die immer verfügbar ist.
Geschäftliche Android-Profile	Gerätefunktionalität	Paket-ID VPN-App	Legen Sie die Paket-ID für die VPN-App fest, die immer verfügbar ist.

Gerätetyp	Gruppe	Name	Beschreibung
Geschäftliche Android-Profile	Gerätefunktionalitä	Verwendung von VPN für geschäftliche Anwendungen erzwingen	Wenn die IT-Richtlinienregel „Verwendung von VPN für geschäftliche Anwendungen erzwingen“ auf das Gerät angewandt wird, wird diese Einstellung ignoriert, und alle geschäftlichen Apps, einschließlich BlackBerry UEM Client und Google Play, dürfen BlackBerry Secure Connect Plus verwenden. In diesem Fall müssen Sie Ports in der Firewall öffnen, damit BlackBerry UEM Client mit BlackBerry Infrastructure über BlackBerry UEM kommunizieren kann. Weitere Informationen zum Öffnen von Ports in der Firewall, wenn geschäftliche Apps BlackBerry Secure Connect Plus verwenden, finden Sie unter http://support.blackberry.com/kb im Artikel KB48330.
Geschäftliche Android-Profile	Gerätefunktionalität	Verwendung von VPN für geschäftliche Daten erzwingen	Legt fest, ob der Benutzer das Gerät in den Sicherheitsmodus booten kann oder nicht. Im Sicherheitsmodus werden alle Drittanbieter-Apps deaktiviert, während vorinstallierte Apps weiterhin funktionieren.
Geschäftliche Android-Profile	Gerätefunktionalitä	Benutzer ermöglichen, im abgesicherten Modus zu starten	Legen Sie fest, ob der Benutzer das Gerät in den Sicherheitsmodus booten kann oder nicht. Im Sicherheitsmodus werden alle Drittanbieter-Apps deaktiviert, während vorinstallierte Apps weiterhin funktionieren.
Geschäftliche Android-Profile	Sicherheit und Datenschutz	Löschen der SD-Karten auf nicht verwaltetem Gerät erzwingen	Wenn das Gerät eine SD-Karte hat, werden die Inhalte darauf beim Zurücksetzen auf Werkseinstellungen, nachdem das Gerät nicht mehr verwaltet wird, gelöscht.
Geschäftliche Android-Profile	Sicherheit und Datenschutz	Rücksetzschutz bei Deaktivierung aufheben	Legen Sie fest, ob der werkseitige Rücksetzschutz bei Deaktivierung des Geräts aufgehoben wird. Wenn Sie diese Regel nicht auswählen und Sie oder ein anderer Benutzer ein Gerät mit aktiviertem werkseitigem Rücksetzschutz deaktivieren, wird das Gerät nach dem Neustart nach dem Google-Kennwort des Benutzers fragen, um das Gerät zu entsperren.

Gerätetyp	Gruppe	Name	Beschreibung
Geschäftliche Android-Profile	Sicherheit und Datenschutz	Benutzer erlauben, Zertifikate zum Zertifikatspeicher des geschäftlichen Bereichs hinzuzufügen	Legen Sie fest, ob der Benutzer im Zertifikatspeicher des geschäftlichen Bereichs vertrauenswürdige Zertifizierungsstellen und Client-Zertifikate hinzufügen kann.
KNOX MDM	Apps	RCS-Funktionen zulassen	Legen Sie fest, ob Rich Communication Services auf dem Gerät verwendet werden können.

Was ist BlackBerry UEM ?

BlackBerry UEM ist eine plattformübergreifende EMM-Lösung von BlackBerry, die umfassende Funktionen für die Verwaltung von Geräten und Anwendungen sowie für das Content Management mit integrierter Sicherheit und Konnektivität bietet und Sie bei der Verwaltung von iOS-, macOS-, Android-, Windows 10-, BlackBerry 10- und BlackBerry OS-Geräten (Version 5.0 bis 7.1) in Ihrem Unternehmen unterstützt.

BlackBerry UEM bietet vertrauenswürdige durchgehende Sicherheit und die für Unternehmen erforderliche Kontrolle, um alle Endpunkte und Eigentümermodelle zu verwalten. Weitere Informationen zum Testen von BlackBerry UEM finden Sie unter blackberry.com.

Funktion	Vorteil
Geringe Gesamtbetriebskosten	BlackBerry UEM reduziert die Komplexität, optimiert die Poolressourcen, sorgt für eine maximale Betriebszeit und unterstützt Sie bei der Erzielung der geringstmöglichen Gesamtbetriebskosten.
Eine einzige webbasierte Schnittstelle	Verwaltung von iOS-, macOS-, Android-, Windows 10- und BlackBerry 10-Geräten 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
Leichtes Einrichten und einfache Anmeldung von Benutzern	Aktivierung benutzereigener Geräte mit BlackBerry UEM Self-Service.
Branchenführende Sicherheit für mobile Geräte	BlackBerry UEM nutzt die BlackBerry Infrastructure, um für Datensicherheit bei allen iOS-, macOS-, Android-, Windows- und BlackBerry-Geräten zu sorgen.
Hohe Verfügbarkeit	Konfiguration von Hochverfügbarkeit, um Dienstunterbrechungen für Gerätebenutzer zu minimieren
Weitere Dienste verfügbar	Enable services such as BlackBerry Workspaces, BlackBerry Enterprise Identity, BlackBerry 2FA, and BlackBerry UEM Notifications that allow you to add value to your BlackBerry UEM Cloud deployment.

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

BlackBerry Enterprise Mobility Suite-Dienste

Neben den Sicherheits- und Produktivitätsfunktionen von BlackBerry UEM bietet BlackBerry weitere Dienste, die den Wert Ihrer BlackBerry UEM-Domäne steigern, um die individuellen Anforderungen Ihres Unternehmens zu

erfüllen. Sie können die nachfolgenden Dienste hinzufügen und sie über die BlackBerry UEM-Verwaltungskonsole verwalten:

Diensttyp	Name und Beschreibung des Dienstes
Enterprise-Dienste	• BlackBerry Workspaces ermöglicht Benutzern das sichere Zugreifen auf, Synchronisieren, Bearbeiten und Freigeben von Dateien und Ordnern auf Windows- und Mac OS-Tablets und -Computern sowie auf Android-, iOS und BlackBerry 10-Geräten. BlackBerry Workspaces schützt Dateien durch die Anwendung von DRM-Steuerelementen, um den Zugriff auch bei gemeinsamer Verwendung außerhalb Ihres Unternehmens einzuschränken. • BlackBerry Enterprise Identity ermöglicht den Zugriff per einmaliger Anmeldung (Single Sign-On, SSO) auf Dienstanbieter wie BlackBerry Workspaces, Box, Workday, WebEx, Salesforce und weitere. Sie können auch Unterstützung für benutzerdefinierte SaaS-Dienste hinzufügen. • BlackBerry 2FA schützt den Zugang auf die kritischen Ressourcen Ihres Unternehmens mithilfe der Zwei-Faktor-Authentifizierung. BlackBerry 2FA fordert ein Kennwort von Benutzern und zeigt jedes Mal eine Sicherheitsaufforderung auf ihrem Android-, iOS- oder BlackBerry 10-Gerät an, wenn diese auf Ressourcen zugreifen möchten. • BlackBerry UEM Notifications ermöglicht Administratoren, direkt von der UEM-Konsole aus Mitteilungen per SMS, Telefon und E-Mail an Benutzer zu senden. Dieses Add-on vereinfacht die Kommunikation mit Endbenutzern und Benutzergruppen, da keine zusätzlichen Messaging-Lösungen erforderlich sind.
BlackBerry Dynamics-Plattform	• Der BlackBerry Enterprise Mobility Server (BEMS) stellt zusätzliche Dienste für BlackBerry Dynamics-Apps bereit. BEMS integriert die folgenden Dienste: BlackBerry Mail, BlackBerry Connect, BlackBerry Presence und BlackBerry Docs. Wenn diese Dienste integriert wurden, können Benutzer über sicheres Instant Messaging miteinander kommunizieren, die Verfügbarkeit von Benutzern in BlackBerry Dynamics-Apps in Echtzeit abrufen und auf geschäftliche Dateiserver und Microsoft SharePoint-Dokumente zugreifen, diese synchronisieren und teilen. • Das BlackBerry Dynamics SDK ermöglicht es den Entwicklern, sichere Apps für Android- und iOS-Geräte sowie Mac OS- und Windows-Computer zu erstellen. Dies ist die Client-Seite der BlackBerry Dynamics-Plattform.

Diensttyp	Name und Beschreibung des Dienstes
BlackBerry Dynamics-Produktivitätsanwendungen	• BlackBerry Workbeinhaltet alles, was Benutzer benötigen, um sicher mobil zu arbeiten, darunter Zugriff auf E-Mails, Kalender und Kontakte (vollständige Synchronisierung mit Microsoft Exchange). Die App ermöglicht zudem erweiterte Zusammenarbeitsfunktionen für Dokumente.BlackBerry Work trennt geschäftliche von persönlichen Daten und kann problemlos auch ohne MDM-Profile auf dem Gerät in andere geschäftliche Apps integriert werden. • BlackBerry Accessermöglicht den Benutzern, von einem beliebigen Mobilgerät über eine sichere Verbindung auf das Intranet des Unternehmens zuzugreifen. • BlackBerry Connectverbessert die Kommunikation und Zusammenarbeit mit sicherem Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen über eine benutzerfreundliche Schnittstelle auf dem Gerät des Benutzers. • BlackBerry Shareermöglicht es Benutzern durch die Integration von Microsoft SharePoint und anderen geschäftlichen Repositories auf den jeweiligen Geräten, über eine sichere Verbindung auf Dokumente zuzugreifen, diese herunterzuladen und zu teilen. • BlackBerry Tasksermöglicht Benutzern, Notizen, die mit Microsoft Exchange auf Android- und iOS-Geräten synchronisiert wurden, zu erstellen, zu bearbeiten und zu verwalten. • BlackBerry Notesermöglicht Benutzern, Notizen, die mit Microsoft Exchange auf einem beliebigen Mobilgerät synchronisiert wurden, zu erstellen, zu bearbeiten und zu verwalten.

Weitere Informationen zu den unterschiedlichen BlackBerry Enterprise Mobility Suite-Lizenzen und zu ihrem Erwerb finden Sie in der Dokumentation zur Lizenzierung.

Vorteile von BlackBerry Workspaces

BlackBerry Workspaces ist eine führende sichere Enterprise File Sync und Share (EFSS)-Lösung (Lösung für Unternehmen zum Synchronisieren und Freigeben von Dateien). Damit können Benutzer überall und jederzeit auf Inhalte zugreifen sowie Dateien innerhalb und außerhalb ihres Unternehmens freigeben. BlackBerry Workspaces beinhaltet einen integrierten Schutz zur Verwaltung von digitalen Rechten (Digital Rights Management, DRM) bei Dateien. Auf diese Weise bleiben Inhalte geschützt und unter Ihrer Kontrolle, auch wenn sie heruntergeladen und freigegeben werden. 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.

Weitere Informationen über die Vorteile von BlackBerry Workspaces finden Sie unter blackberry.com.

Vorteile von BlackBerry Enterprise Identity

BlackBerry Enterprise Identity erleichtert Benutzern den Zugriff auf Cloud-Anwendungen von jedem Gerät, wie iOS, Android und BlackBerry sowie von herkömmlichen Rechnerplattformen. 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 wird in der BlackBerry Enterprise Mobility Suite – Application Edition und BlackBerry Enterprise Mobility Suite - Content Edition angeboten.

Weitere Informationen zu den Vorteilen von BlackBerry Enterprise Identity finden Sie unter blackberry.com.

Vorteile von BlackBerry 2FA

BlackBerry 2FA bietet eine Zwei-Faktor-Authentifizierung über ein Kennwort sowie das Gerät des Benutzers und nutzt Ihre vorhandenen iOS-, Android- oder BlackBerry-Geräte, um für ein unkompliziertes Anwendererlebnis zu sorgen und zudem die Sicherheit in Ihrem Unternehmen zu verbessern.

BlackBerry 2FA wird in der BlackBerry Enterprise Mobility Suite – Application Edition und BlackBerry Enterprise Mobility Suite - Content Edition angeboten.

Weitere Informationen zu den Vorteilen von BlackBerry 2FA finden Sie unter blackberry.com.

Vorteile von BlackBerry UEM Notifications

BlackBerry UEM Notifications vereinfacht die Kommunikation mit Endbenutzern und Benutzergruppen. Administratoren können von der UEM-Verwaltungskonsole wichtige Benachrichtigungen an Benutzer senden.

Da UEM Notifications Administratoren erlaubt, Geräte und Benachrichtigungen in der UEM-Verwaltungskonsole zu verwalten, müssen sie Kontaktinformationen der Benutzer nicht auf mehreren Systemen verwalten und abgleichen oder sich mit Zugriffsproblemen in externen Systemen befassen. UEM Notifications verwendet Kontaktinformationen mithilfe der Microsoft Active Directory-Synchronisation. UEM Notifications bietet zudem flexible Bereitstellungsoptionen wie 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.

Weitere Informationen zu UEM Notifications finden Sie in UEM Benachrichtigungsinhalt.

Wichtigste BlackBerry UEM Funktionen

Funktion	Beschreibung
Plattformübergreifende Geräteverwaltung	Sie können Geräte mit iOS, macOS, Android, Windows und BlackBerry verwalten.
Einheitliche, intuitiv bedienbare Benutzeroberfläche	Sie können alle Geräte an einem Ort anzeigen und über eine einzige webbasierte Benutzeroberfläche auf alle Verwaltungsaufgaben zugreifen. Sie können Verwaltungsaufgaben gemeinsam mit anderen Administratoren erledigen, die gleichzeitig auf die Verwaltungskonsole zugreifen können. Sie können zwischen Standard- und erweiterten Ansichten umschalten, um Optionen für die Anzeige von Informationen und das Filtern der Benutzerliste zu sehen.
Bewährtes, sicheres Benutzererlebnis	Die Gerätesteuerungen ermöglichen eine präzise Verwaltung der Verbindung von Geräten mit dem Netzwerk, der aktivierten Leistungsmerkmale und der verfügbaren Apps. Ob die Geräte nun Eigentum Ihres Unternehmens oder Ihrer Benutzer sind, Sie können in jedem Fall die Daten Ihres Unternehmens schützen.
Trennung geschäftlicher und persönlicher Anforderungen	Sie können Geräte mit Android-Arbeitsprofilen, Samsung KNOX- und BlackBerry Balance-Technologien verwalten, die darauf abzielen, persönliche und geschäftliche Informationen auf den Geräten zu trennen und sichern. Wenn ein Gerät verloren geht oder der Mitarbeiter das Unternehmen verlässt, können Sie nur die geschäftlichen oder alle Daten vom Gerät löschen. Das Plug-In WorkLife von BlackBerry wird über die BlackBerry UEM-Verwaltungskonsole verwaltet. WorkLife von BlackBerry ist eine virtuelle SIM-Plattform (VSP), mit deren Hilfe geschäftliche und persönliche Nummern auf BlackBerry 10-, iOS- und Android-Geräten voneinander getrennt werden können. Weitere Informationen über die Installation und Verwaltung von WorkLife in BlackBerry finden Sie in der Dokumentation zu WorkLife von BlackBerry .
Sichere IP-Konnektivität	Mit BlackBerry Secure Connect Plus können Sie einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf BlackBerry 10-, iOS-, Samsung KNOX Workspace- und Android-Geräten mit Arbeitsprofil und dem Netzwerk des Unternehmens bereitstellen. Über diesen Tunnel haben Benutzer Zugriff auf Ressourcen hinter der Firewall des Unternehmens, wobei die Sicherheit der Daten mithilfe standardmäßiger IPv4-Protokolle (TCP und UDP) und durchgehender Verschlüsselung sichergestellt wird.

Funktion	Beschreibung
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.
Integration in Dienste wie beispielsweise BlackBerry Workspaces,BlackBerry Enterprise Identity, BlackBerry 2FA und BlackBerry UEM Notifications	Sie können BlackBerry UEM in BlackBerry Workspaces,BlackBerry Enterprise Identity, BlackBerry 2FA und BlackBerry UEM Notifications integrieren, mit denen Sie den Wert der BlackBerry UEM-Instanz Ihres Unternehmens steigern können.
Leistungsstarke App-Verwaltung	BlackBerry UEM ist eine umfassende App-Verwaltungsplattform für alle Geräte. Sie können Apps aus allen wichtigen App Stores, einschließlich App Store, Google Play, Windows Store und BlackBerry World-Storefront, bereitstellen.
Rollenbasierte Verwaltung	Sie können Verwaltungsaufgaben für andere Administratoren freigeben, die gleichzeitig auf die Administrationskonsolen zugreifen können. Sie können mithilfe von Rollen die Aktionen definieren, die ein Administrator ausführen kann, und durch die Beschränkung der Optionen für die einzelnen Administratoren Sicherheitsrisiken senken, Aufgaben verteilen und die Effizienz erhöhen. Sie können vordefinierte Rollen verwenden oder eigene Rollen erstellen.
Integration des Unternehmensverzeichnisses	Sie können eine lokale, integrierte Benutzerauthentifizierung verwenden, um auf die Verwaltungskonsole und die Selbstbedienungskonsole zuzugreifen, oder Sie können die Authentifizierung in Microsoft Active Directory oder den in der Unternehmensumgebung verwendeten LDAP-Unternehmens-verzeichnissen (beispielsweise IBM Domino Directory) integrieren. BlackBerry UEM unterstützt Verbindungen mit mehreren Verzeichnissen. Sie können eine beliebige Kombination von Microsoft Active Directory und LDAP verwenden. 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. 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.

Funktion	Beschreibung
Cisco ISE-Integration	Cisco Identity Services Engine (ISE) ist eine Software zur Netzwerkverwaltung, die einem Unternehmen die Möglichkeit bietet, den Zugriff von Geräten auf das Unternehmensnetzwerk zu steuern (z. B. Zugriff auf Wi-Fi- oder VPN-Verbindungen zulassen oder verweigern). In dieser Version können Sie eine Verbindung zwischen Cisco ISE und BlackBerry UEM herstellen, damit Cisco ISE Daten über die Geräte abrufen kann, die in BlackBerry UEM aktiviert sind. Cisco ISE prüft die Gerätedaten, um zu bestimmen, ob Geräte den Zugriffsrichtlinien Ihres Unternehmens entsprechen.
Synchronisieren mit einem Good Control-Server	Nach der Installation von BlackBerry UEM Version 12.7 in einer Umgebung mit einem bestehenden Good Control-Server müssen Sie Good Control mit BlackBerry UEM synchronisieren, um die Funktionen von BlackBerry UEM Version 12.7 zu aktivieren.
Regionale Bereitstellung	Sie können regionale Verbindungen für Unternehmensverbindungsfunktionen einrichten, indem Sie BlackBerry Connectivity Node-Instanzen in einer bestimmten Region bereitstellen. Dies wird auch als Servergruppe bezeichnet. Jeder BlackBerry Connectivity Node umfasst BlackBerry Secure Connect Plus, den BlackBerry Gatekeeping Service, den BlackBerry Secure Gateway, BlackBerry Proxy und den BlackBerry Cloud Connector. Sie können einer Servergruppe Profile für Unternehmensverbindungen und E-Mail-Funktionen zuordnen, sodass alle Benutzer, die eine Zuordnung dieser Profile aufweisen, eine bestimmte regionale Verbindung zur BlackBerry Infrastructure bei Verwendung von BlackBerry Connectivity Node-Komponenten nutzen. Durch die Bereitstellung von mehr als einem BlackBerry Connectivity Node in einer Servergruppe wird eine hohe Verfügbarkeit und Lastverteilung erzielt.
Wearable-Geräte	Sie können bestimmte Android-basierte, am Kopf tragbare Geräte in BlackBerry UEM aktivieren und verwalten. Zum Beispiel können Sie Vuzix M300 Smart Glasses verwalten. Intelligente Brillen ermöglichen den berührungslosen Zugriff auf visuelle Informationen, wie z. B. Benachrichtigungen, Schritt-für-Schritt-Anleitungen, Bilder und Videos, die Nutzung von Sprachsteuerung und GPS-Navigation oder das Scannen von Barcodes. Beispiele für BlackBerry UEM-Verwaltungsfunktionen, die unterstützt werden, umfassen: Geräteaktivierung mit QR-Code, IT-Richtlinien, Wi-Fi- und VPN-Profile, App-Management und standortbezogene Dienste.

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

Schlüsselmerkmale aller Gerätetypen

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

Funktion	Beschreibung
Aktivieren von Geräten	Wenn Sie ein Gerät aktivieren, weisen Sie das Gerät Ihrer Unternehmensumgebung zu, damit Benutzer auf ihren Geräten auf Geschäftsdaten zugreifen können. Sie können ein Gerät einfach nur mit einer E-Mail-Adresse und einem Aktivierungskennwort aktivieren. 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.
Verwalten von Geräten	Sie können alle Geräte an einem Ort anzeigen und über eine einzige webbasierte Benutzeroberfläche auf alle Verwaltungsaufgaben zugreifen. Sie können mehrere Geräte für jedes Benutzerkonto verwalten und den Gerätbestand Ihres Unternehmens anzeigen. Sie können die folgenden Aktionen durchführen, sofern diese vom Gerät unterstützt werden: • 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	Mithilfe von Gruppen wird die Verwaltung von Benutzern, Apps und Geräten vereinfacht. Sie können Gruppen dazu verwenden, um die gleichen Konfigurationseinstellungen auf ähnliche Benutzerkonten oder Geräte anzuwenden. Sie können unterschiedliche App-Gruppen zu verschiedenen Benutzergruppen zuweisen, und ein Benutzer kann Mitglied mehrerer Gruppen sein.

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

Funktion	Beschreibung
Zertifikatsbasierte Authentifizierung	Sie können Zertifikate mithilfe von Zertifikatsprofilen an Geräte senden. Diese Profile helfen dabei, den Zugriff auf Microsoft Exchange ActiveSync-, Wi-Fi- oder VPN-Verbindungen auf Geräte zu beschränken, die eine zertifikatsbasierte Authentifizierung nutzen.
Verwalten von Lizenzen für bestimmte Funktionen und Gerätesteuerungen	Sie können für die einzelnen Lizenztypen die Lizenzen verwalten und detaillierte Informationen anzeigen, wie etwa zu Nutzungs- und Ablaufdaten. Durch die von Ihrem Unternehmen verwendeten Lizenztypen werden die Geräte und Funktionen bestimmt, die Sie verwalten können. Sie müssen Lizenzen aktivieren, bevor Sie Geräte aktivieren können. Es stehen kostenlose Testversionen zur Verfügung, sodass Sie den Dienst ausprobieren können.
EMM SIM-Based Licensing	Die EMM SIM-basierte Lizenzierung ist ein alternatives Lizenzierungsmodell, bei dem Sie Lizenzen von Ihrem Dienstanbieter anstatt von BlackBerry erwerben. Bei dieser Option können Sie die Lizenzen für BlackBerry 10-, iOS-, Android- und Windows-Geräte im Rahmen Ihres bestehenden Tarifs bei Ihrem Dienstanbieter bezahlen. Weitere Informationen zur Lizenzierung finden Sie in der Dokumentation zur Lizenzierung.

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 Webinhalt auf Geräten mit iOS 7 und Nachfolgeversionen	Für Geräte mit iOS 7.0 und höher können Sie Webinhaltsfilter-Profile verwenden, um die Websites einzuschränken, die der Benutzer auf dem Gerät anzeigen kann. Sie können das automatische Filtern mit der Option zum Zulassen und Einschränken von Websites aktivieren oder den Zugriff nur auf bestimmte Websites zulassen.
Verknüpfen von Apple VPP-Konten mit einer BlackBerry UEM-Domäne	VPP (Volume Purchase Program) ermöglicht Ihnen, iOS-Apps in Mengen zu kaufen und zu verteilen. Sie können Apple VPP-Konten mit einer BlackBerry UEM-Domäne verknüpfen, sodass Sie gekaufte Lizenzen für mit VPP-Konten verknüpfte iOS-Apps verteilen können.
Programm zur Geräteregistrierung (DEP) von Apple	Sie können BlackBerry UEM für die Verwendung des Programms zur Geräteregistrierung (DEP) von Apple konfigurieren, damit Sie BlackBerry UEM mit DEP synchronisieren können. Nach der Konfiguration von BlackBerry UEM können Sie die Aktivierung der von Ihrem Unternehmen für DEP erworbenen iOS-Geräte mit der BlackBerry UEM-Verwaltungskonsole verwalten. Sie können mehrere DEP-Konten verwenden. Sie können mehrere Apple-DEP-Konten mit einer BlackBerry UEM-Domäne verknüpfen. Weitere Informationen zum Konfigurieren von BlackBerry UEM und zum Aktivieren von iOS-Geräten, die bei dem Programm für die Geräteregistrierung (DEP) registriert sind, finden Sie in der Dokumentation zur Konfiguration und in der Dokumentation für Administratoren.
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. Diese Option wird nur für iOS-Geräte unterstützt.

Funktion	Beschreibung
Verwenden benutzerdefinierterPayload-Profile	Mit benutzerdefinierten Payload-Profilen können Sie Funktionen auf iOS-Geräten steuern, die nicht durch bestehende BlackBerry UEM-Richtlinien oder -Profile gesteuert werden. Sie können mit Apple Configurator Apple-Konfigurationsprofile erstellen und diese den benutzerdefinierten BlackBerry UEM-Payload-Profilen hinzufügen. Sie können benutzerdefinierte Payload-Profile Benutzern, Benutzergruppen und Gerätegruppen zuweisen.
BlackBerry Secure Gateway	Der BlackBerry Secure Gateway ermöglicht iOS-Geräten mit der Aktivierungsart „MDM-Steuerelemente“ die Verbindung zu einem geschäftlichen E-Mail-Server über die BlackBerry Infrastructure und BlackBerry UEM. Wenn Sie den BlackBerry Secure Gateway verwenden, müssen Sie Ihren E-Mail-Server nicht außerhalb der Firewall verfügbar machen, damit Benutzer dieser Geräte geschäftliche E-Mails empfangen können, wenn keine Verbindung zum VPN Ihres Unternehmens oder dem geschäftlichen Wi-Fi-Netzwerk besteht.
Integration mit BlackBerry Dynamics	Sie können das BlackBerry Dynamics-Profil verwenden, um iOS-Geräten den Zugriff auf BlackBerry Dynamics-Produktivität-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect zu ermöglichen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen das BlackBerry Dynamics-Profil zuweisen. Mehrere Geräte können auf dieselben Apps zugreifen. Das Profil ermöglicht die Aktivierung von BlackBerry Dynamics für Benutzer, die bereits für BlackBerry Dynamics aktiviert sind.
Per-App-VPN	Sie können ein Per-App-VPN für iOS-Geräte einrichten, um anzugeben, welche Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Ein Per-App-VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (z. B. Zugriff auf Anwendungsserver oder Webseiten hinter der Firewall). Diese Funktion unterstützt auch die Privatsphäre des Benutzers und erhöht die Verbindungsgeschwindigkeit für persönliche Apps, indem der persönliche Datenverkehr nicht über das VPN gesendet wird. Für iOS-Geräte sind Apps mit einem VPN-Profil verknüpft, wenn Sie die App oder App-Gruppe einem Benutzer, einer Benutzergruppe oder einer Gerätegruppe zuweisen.
Apple-Aktivierungssperre	Für die Funktion „Aktivierungssperre“ auf iOS 7 und höher sind Apple-ID und Kennwort des Benutzers erforderlich, bevor ein Benutzer „Mein iPhone suchen“ deaktivieren, das Gerät löschen oder reaktivieren und verwenden kann. Sie können die Aktivierungssperre umgehen, um ein COPE- oder COBO-Gerät einem anderen Benutzer zur Verfügung zu stellen.
Persönliche App-Listen	Sie können eine Liste der Apps anzeigen, die im persönlichen Bereich des Benutzers auf iOS-Geräten in Ihrer Umgebung installiert sind. Sie können über die Seite „Benutzerdetails“ eine Liste der auf dem Gerät eines Benutzers installierten persönlichen Apps anzeigen, oder Sie können über die Seite „Persönliche Apps“ in der Verwaltungskonsole eine Liste aller persönlichen Apps anzeigen, die in persönlichen Bereichen der Benutzer installiert sind.

Funktion	Beschreibung
Verloren-Modus für überwachte iOS-Geräte	Der Verloren-Modus ermöglicht das Sperren eines Geräts, das Festlegen einer anzuzeigenden Nachricht und das Anzeigen des aktuellen Standorts eines verloren gegangenen Geräts. Sie können den Verloren-Modus für überwachte iOS-Geräte mit iOS Version 9.3 oder höher aktivieren.
IBM Notes Traveler-Unterstützung	iOS-Geräte können nun eine Verbindung zu IBM Notes Traveler über den BlackBerry Secure Gateway herstellen.
Face ID-Unterstützung	BlackBerry UEM unterstützt die Face ID für die Authentifizierung von Geräten und zum Öffnen von BlackBerry Dynamics-Apps.
Management freigegebener Geräte	Sie können zulassen, dass mehrere Benutzer ein iOS-Gerät gemeinsam verwenden. Sie können die Nutzungsbestimmungen anpassen, die Benutzer akzeptieren müssen, um freigegebene Geräte abzumelden. Ein Benutzer kann ein Gerät per lokaler Authentifizierung abmelden und sobald er fertig ist wieder anmelden, damit es für den nächsten Benutzer zur Verfügung steht. Freigegebene Geräte werden während des Abmeldungs- und Anmeldungsprozesses von BlackBerry UEM verwaltet. Diese Funktion wurde speziell für überwachte Geräte mit der folgenden Konfiguration entwickelt: • App-Sperrmodus aktiviert • VPP-Apps zugewiesen

Android-Geräte

Funktion	Beschreibung
Geräte mit Android MDM verwalten	Android MDM uses the basic management options that are native to the Android OS to manage the device. A separate, protected container is not created. For more information about managing devices using Android MDM, finden Sie in der Dokumentation für Administratoren.

Funktion	Beschreibung
Verwalten von Geräten mit KNOX MDM und KNOX Workspace	BlackBerry UEM kann Samsung-Geräte mithilfe von Samsung KNOX MDM und Samsung KNOX Workspace verwalten. KNOX Workspace bietet einen verschlüsselten kennwortgeschützten Container auf einem Samsung-Gerät für geschäftliche Apps und Daten. Er trennt die persönlichen Apps und Daten eines Benutzers von denen des Unternehmens und schützt letztere mithilfe erweiterter, von Samsung entwickelter Sicherheits- und Verwaltungsfunktionen. 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: • Erweiterte IT-Richtlinienregeln • Erweiterte Anwendungsverwaltung, einschließlich automatischer Installation und Deinstallation von Apps, automatischer Deinstallation gesperrter Apps und Verhinderung der Installation gesperrter Apps • App-Sperrmodus Weitere Informationen zu den unterstützten Geräten finden Sie in der Kompatibilitätsmatrix. Weitere Informationen zu KNOX finden Sie unter https://www.samsungknox.com. Weitere Informationen zur Verwaltung von Geräten mit KNOX finden Sie in der Dokumentation für Administratoren.
Verwalten von Geräten, auf denen Android-Arbeitsprofile verwendet werden	Sie können Android-Geräte, auf denen Android OS 5.1 oder höher ausgeführt wird, für die Verwendung von Android-Arbeitsprofilen aktivieren. Android-Arbeitsprofile sind eine von Google entwickelte Funktion, die zusätzliche Sicherheit für Unternehmen bietet, die Android-Geräte verwalten und die Verwendung ihrer Daten und Apps auf Android-Geräten zulassen möchten. Weitere Informationen zur Verwaltung von Geräten mit Android-Arbeitsprofilen finden Sie in der Dokumentation für Administratoren.
Integration mit BlackBerry Dynamics	Sie können das BlackBerry Dynamics-Profil verwenden, um Android-Geräten den Zugriff auf BlackBerry Dynamics-Produktivität-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect zu ermöglichen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen das BlackBerry Dynamics-Profil zuweisen. Mehrere Geräte können auf dieselben Apps zugreifen. Das Profil ermöglicht die Aktivierung von BlackBerry Dynamics für Benutzer, die bereits für BlackBerry Dynamics aktiviert sind.
Per-App-VPN	Sie können „Per App VPN“ für Android-Geräte mit Arbeitsprofil aktivieren, um die Verwendung von BlackBerry Secure Connect Plus auf bestimmte geschäftliche Apps zu beschränken, die Sie einer Positivliste hinzufügen.

Funktion	Beschreibung
Zero-Touch-Registrierung	BlackBerry UEM unterstützt nur 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.
Derived smart credentials	Use Entrust IdentityGuard derived smart credentials for signing, encryption, and authentication for BlackBerry Dynamics apps and apps in the work space on Android work profile and Samsung KNOX Workspace devices.

Windows-Geräte

Funktion	Beschreibung
Unterstützung für Windows 10-Geräte	Sie können Windows 10-Geräte – Windows 10-Mobilgeräte und Windows 10-Tablets und -Computer – verwalten. Silver-Lizenzen sind zur Aktivierung von Windows 10-Geräten erforderlich.
Proxyunterstützung für Windows 10-Geräte	Sie können VPN- und geschäftliche WLAN-Verbindungen für Windows 10-Geräte konfigurieren und einen Proxyserver als Teil des Wi-Fi-Profils Windows 10 Mobile- für Geräte einrichten.
Per-App-VPN	Sie können ein Per-App-VPN für Windows 10-Geräte einrichten, um anzugeben, welche Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Ein Per-App-VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (z. B. Zugriff auf Anwendungsserver oder Webseiten hinter der Firewall). Diese Funktion unterstützt auch die Privatsphäre des Benutzers und erhöht die Verbindungsgeschwindigkeit für persönliche Apps, indem der persönliche Datenverkehr nicht über das VPN gesendet wird. Für Windows 10-Geräte werden im VPN-Profil Apps der App-Auslöserliste hinzugefügt.
Windows-Datenschutz für Windows 10-Geräte	Sie können Windows-Datenschutzprofile konfigurieren, um persönliche Daten und geschäftliche Daten auf Geräten getrennt voneinander zu halten, um Benutzer daran zu hindern, geschäftliche Daten außerhalb von geschützten geschäftlichen Apps freizugeben oder mit Personen außerhalb des Unternehmens zu teilen und um unangemessene Methoden zum Teilen von Daten zu überwachen. Sie können angeben, welche Apps geschützt sind und welchen Apps vertraut wird, um geschäftliche Dateien zu erstellen und darauf zuzugreifen.

BlackBerry 10-Geräte

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

Vergleich von BlackBerry UEM mit vorherigen EMM-Lösungen von BlackBerry

EMM-Lösung	Unterstützte Gerätetypen	Beschreibung
BlackBerry UEM	• BlackBerry 10 • BlackBerry OS (Version 5.0 bis 7.1) • iOS (einschließlich DEP-Geräte) • macOS • Android (einschließlich Geräte mit Arbeitsprofil und Samsung KNOX) • Windows Phone • Windows 10 • Windows 10 Mobile	Eine plattformübergreifende EMM-Lösung, die Ihnen die Verwaltung des Servers, der Benutzerkonten und aller Gerätetypen über eine einzige Benutzeroberfläche ermöglicht. Diese einfache, webbasierte Verwaltungskonsole ermöglicht Ihnen die Verwaltung von BYOD-, COPE- und COBO-Geräten sowie den Schutz von Geschäftsinformationen. Die Softwarearchitektur wurde vereinfacht und ermöglicht nun eine einfachere Verwaltung, eine verbesserte Skalierbarkeit und zusätzliche Multi-Plattform-Funktionen. Um eine hohe Verfügbarkeit zu erzielen, können Sie zusätzliche aktive Server installieren, die die Verwaltungslast automatisch verteilen. Hinweis: Zur Verwaltung von BlackBerry-Geräten (Version 5.0 bis 7.1) mit BlackBerry UEM müssen Sie ein Upgrade von BES5 auf BlackBerry UEM durchführen.
BES10	• iOS • Android • BlackBerry 10 • BlackBerry OS (Version 5.0 bis 7.1)	Sie können die Server, Geräte und Benutzerkonten über spezielle erweiterte Benutzeroberflächen für die verschiedenen Gerätetypen verwalten. Zusätzlich können Sie BlackBerry Management Studio als einzelne, vereinheitlichte Benutzeroberfläche für die grundlegende Administration aller Geräte verwenden. Um eine hohe Verfügbarkeit sicherzustellen, haben Sie die Möglichkeit, Standby-Instanzen des Servers zu installieren. Zur Verwaltung von Geräten mit BlackBerry OS (Version 5.0 bis 7.1) können Sie BES10 auf dem gleichen Computer installieren wie BlackBerry Enterprise Server 5.0 SP4 und BlackBerry Management Studio für die grundlegende Verwaltung verwenden.
BES5 5	• BlackBerry OS (Version 5.0 bis 7.1)	Sie können den Server, die Geräte und die Benutzerkonten über den BlackBerry Administration Service verwalten. Um eine hohe Verfügbarkeit sicherzustellen, können Standby-Instanzen der meisten Serverkomponenten installiert werden.

Produktunterlagen

Ressource	Beschreibung
Übersicht und neue Funktionen	• Einführung in den BlackBerry UEM und seine Leistungsmerkmale • Neuheiten
Architektur und Datenflüsse	• Architektur • Beschreibung der BlackBerry UEM-Komponenten • Beschreibung der Aktivierung und anderer Datenflüsse, wie Konfigurationsupdates und E-Mail, für unterschiedliche Gerätetypen
Versionshinweise und Ratgeber	• Beschreibung behobener Probleme • Beschreibung von bekannten Problemen und potenziellen Workarounds • Neuheiten
Installation und Upgrade	• Systemanforderungen • Installationsanweisungen • Upgrade-Anweisungen
Planung	• Planen der Bereitstellung von BlackBerry UEM für eine Installation oder ein Upgrade von BES5 oder BES10
Lizenzierung	• Anweisungen zum Erhalt, zur Aktivierung und Verwaltung von Lizenzen • Beschreibung der verschiedenen Lizenztypen • Anweisungen zur Aktivierung und Verwaltung von Lizenzen
Konfiguration	• Anweisungen zur Konfiguration von Serverkomponenten vor Beginn der Verwaltung von Benutzern und deren Geräten • Anweisungen zur Migration von Daten aus einer bestehenden BES10- oder BlackBerry UEM-Datenbank
Verwaltung	• Grundlegende und erweiterte Verwaltung der unterstützten Gerätetypen. Dazu gehören Geräte mit folgenden Plattformen: BlackBerry 10, iOS, macOS, Android, Windows und BlackBerry OS (Version 5.0 bis 7.1) sowie frühere Versionen • Anweisungen zum Erstellen von Benutzerkonten, Gruppen, Rollen und Administratorkonten • Anweisungen zur Aktivierung von Geräten • Anweisungen zum Erstellen und Zuweisen von IT-Richtlinien und Profilen • Anweisungen zum Verwalten von Apps auf Geräten • Beschreibung der Profileinstellungen • Beschreibung der IT-Richtlinienregeln für Geräte mit folgenden Plattformen: BlackBerry 10, iOS, macOS, Android, Windows und BlackBerry OS (Version 5.0 bis 7.1) sowie frühere Versionen

Ressource	Beschreibung
Sicherheit	• Beschreibung von Gerätesicherheitsfunktionen • Beschreibung, wie Sie BlackBerry UEM verwenden können, um Gerätesicherheitsfunktionen wie Verschlüsselung, Kennwörter und Datenbereinigung zu verwalten • Beschreibung, wie BlackBerry UEM Daten während der Übertragung zwischen Geräten, der BlackBerry Infrastructure, BlackBerry UEM und den Ressourcen Ihrer Organisation schützt
Kompatibilitätsmatrix	• Liste der unterstützten Betriebssysteme, Datenbankserver und Browser für den BlackBerry UEM-Server • Liste der unterstützten Samsung KNOX-Betriebssysteme • Liste der unterstützten Android-Betriebssysteme
Häufig gestellte Fragen	• Antworten auf häufig gestellte Fragen zu unterschiedlichen Themen, z. B. Verwaltung, Lizenzierung und Zertifikaten
BlackBerry Enterprise Produkte	• Beschreibung von BlackBerry-Produkten, wie z. B. BlackBerry UEM, BlackBerry UEM Cloud, Strong Authentication by BlackBerry, Enterprise Identity by BlackBerry und BlackBerry Workspaces