BlackBerry UEM

Übersicht und Architektur

12.19

Contents

Was ist BlackBerry UEM?

BlackBerry UEM ist eine plattformübergreifende EMM-Lösung, 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-Geräten in Ihrem Unternehmen unterstützt.

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

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

Zu den Vorteilen von UEM zählen:

Funktion	Vorteil
Geringe Gesamtbetriebskosten	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. 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-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 auf UEM 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 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 UEM Notifications, mit denen Sie den Wert IhrerUEM-Bereitstellung steigern können.

Wichtigste Funktionen von BlackBerry UEM

Funktion	Beschreibung
Plattformübergreifende Geräteverwaltung	Sie können Geräte mit iOS, macOS, Android und Windows verwalten.
Einheitliche, intuitiv bedienbare Benutzeroberfläche	Sie können alle Geräte an einem Ort anzeigen und alle Verwaltungsaufgaben über eine einzelne webbasierte Benutzerschnittstelle aufrufen. Sie können Aufgaben für mehrere Administratoren freigeben, die gleichzeitig auf die Verwaltungskonsole zugreifen können. Sie können zwischen Standard- und erweiterten Ansichten umschalten, um Optionen für die Anzeige von Informationen und das Filtern der Benutzerliste zu sehen.
Zuverlässige und sichere Benutzererfahrung	Steuerungsfunktionen für Geräte ermöglichen eine präzise Verwaltung der Verbindung von Geräten mit dem Netzwerk, der aktivierten Funktionen und der verfügbaren Apps. Die Unternehmensdaten werden geschützt, ungeachtet dessen, ob die Geräte sich im Besitz Ihres Unternehmens oder Ihrer Benutzer befinden.
Trennung geschäftlicher und persönlicher Anforderungen	Sie können Geräte mit Android Enterprise-, Android Management- und Samsung Knox-Technologien verwalten, die darauf abzielen, persönliche und geschäftliche Informationen auf den Geräten zu trennen und sichern. Wenn ein Gerät verloren geht oder kompromittiert wird, 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. Mit UEM Self-Service können Benutzer Geräte aktivieren oder wechseln, ihr Gerätekennwort per Fernzugriff ändern, Gerätedaten löschen oder ein verlorenes oder gestohlenes Gerät sperren.
Integration mit anderen BlackBerry-Diensten	Sie können UEM mit BlackBerry Workspaces, BlackBerry Enterprise Identity und BlackBerry 2FA integrieren und dadurch den Wert der UEM-Instanz Ihres Unternehmens steigern.
Leistungsstarke App-Verwaltung	UEM ist eine umfassende App-Verwaltungsplattform für alle Geräte. Sie können Apps aus allen wichtigen App Stores, einschließlich App Store und Google Play bereitstellen.

Funktion	Beschreibung
Rollenbasierte Verwaltung	Sie können Aufgaben für mehrere Administratoren freigeben, die gleichzeitig auf die Verwaltungskonsole zugreifen können. Sie können mithilfe von Rollen die Aktionen definieren, die ein Administrator ausführen kann, und die 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 UEM mit Microsoft Active Directory, LDAP oder Entra ID-Verzeichnissen integrieren, die Sie in der Unternehmensumgebung verwenden. UEM unterstützt Verbindungen mit mehreren Verzeichnissen. Sie können Benutzerkonten in UEM mithilfe von Benutzerdaten aus dem Verzeichnis erstellen und Unternehmensverzeichnisgruppen mit UEM verknüpfen, um Benutzer in UEM auf die gleiche Weise zu organisieren, wie sie in Ihrem Unternehmensverzeichnis organisiert sind. Sie haben auch die Möglichkeit, für bestimmte Gruppen in Ihrem Unternehmensverzeichnis Onboarding zu aktivieren, um UEM-Benutzer automatisch erstellen zu lassen. Wenn Sie Onboarding aktivieren, können Sie mithilfe von Offboarding-Konfigurationen auch Gerätedaten oder Benutzerkonten löschen, wenn Benutzer aus Gruppen in Ihrem Unternehmensverzeichnis entfernt werden.
Migration	Sie können Benutzer, Geräte, Gruppen und andere Daten von einer lokalen UEM-Quelldatenbank auf eine neue lokale oder UEM Cloud-Instanz migrieren.
Cisco ISE-Integration	Cisco Identity Services Engine (ISE) ist eine Software zur Netzwerkverwaltung, die einem Unternehmen die Möglichkeit bietet, den Zugriff von Geräten auf das Unternehmensnetzwerk zu steuern (z. B. Zugriff auf Wi-Fi- oder VPN-Verbindungen zulassen oder verweigern). Sie können eine Verbindung zwischen Cisco ISE und UEM (lokal) herstellen, damit Cisco ISE auf Daten von Geräten zugreifen kann, die auf UEM aktiviert sind. Cisco ISE prüft die Gerätedaten, um zu bestimmen, ob Geräte den Zugriffsrichtlinien Ihres Unternehmens entsprechen.

Funktion	Beschreibung
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 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.
Wearable-Geräte	Sie können bestimmte Wearables auf Android-Basis in 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 UEM-Verwaltungsfunktionen, die unterstützt werden, umfassen: Geräteaktivierung mit QR-Code, IT-Richtlinien, Wi-Fi- und VPN-Profile, App-Management und standortbezogene Dienste.
Microsoft Intune-Integration	Bei iOS- und Android-Geräten, 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 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.

Schlüsselmerkmale aller Gerätetypen

Funktion	Beschreibung
Aktivieren von Geräten	Wenn Benutzer ein Gerät aktivieren, verbinden sie es mit UEM und mit ihrer Unternehmensumgebung, damit Sie mit dem Gerät auf geschäftliche Daten zugreifen können. Benutzer können ihre Geräte mit einem QR-Code oder ihrer 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 an sie verteilen. Alle Gerätetypen können über das Mobilfunknetz aktiviert werden.

Funktion	Beschreibung
Geräte verwalten	Sie können alle Geräte anzeigen und alle Verwaltungsaufgaben über eine einzelne webbasierte Konsole aufrufen. Sie können mehrere Geräte für jedes Benutzerkonto verwalten und den Gerätbestand Ihres Unternehmens anzeigen. Sie können die folgenden Aktionen ausführen, wenn sie 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.
Steuern, welche Geräte Zugriff auf Microsoft Exchange ActiveSync erhalten	Mit Gatekeeping können Sie sicherstellen, dass nur von UEM verwaltete Geräte auf geschäftliche 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 UEM an Port 3101.

Funktion	Beschreibung
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.
Durchsetzen von Geräteanforderungen Ihres Unternehmens	Mithilfe eines Konformitätsprofils können Sie dazu beitragen, dass die Sicherheitsanforderungen Ihres Unternehmens 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.
Erstellen oder Importieren von vielen Benutzerkonten mit einer .csv-Datei	Sie können eine CSV-Datei in 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 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.
Hohe Verfügbarkeit und Notfallwiederherstellung	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. BlackBerry-Rechenzentren verfügen über Pläne zur Notfallwiederherstellung bei Ausfällen von Diensten. Die Pläne sind so konzipiert, dass sie eine minimale Auswirkung auf die Benutzer der Geräte haben und dass die Kontinuität des Geschäfts sichergestellt wird. Daten und Anwendungen werden nahezu in Echtzeit gesichert, um Datenverlust zu vermeiden.
Zertifikatsbasierte Authentifizierung	Sie können Zertifikate mithilfe von Zertifikatsprofilen an Geräte senden. Diese Profile helfen dabei, den Zugriff auf Microsoft Exchange ActiveSync-, Wi-Fi- oder VPN-Verbindungen auf Geräte zu beschränken, die eine zertifikatsbasierte Authentifizierung nutzen.

Funktion	Beschreibung
Verwalten von Lizenzen für bestimmte Funktionen und Gerätesteuerungen	Sie können für die einzelnen Lizenztypen die Lizenzen verwalten und detaillierte Informationen anzeigen, wie etwa zu Nutzungs- und Ablaufdaten. Durch die von Ihrem Unternehmen verwendeten Lizenztypen werden die Geräte und Funktionen bestimmt, die Sie verwalten können. Sie müssen Lizenzen aktivieren, bevor Sie Geräte aktivieren können. Es stehen kostenlose Testversionen zur Verfügung, sodass Sie den Dienst ausprobieren können.

Schlüsselmerkmale der einzelnen Gerätetypen

iOS-Geräte

Funktion	Beschreibung
Geräteaktivierung	Mit dem Apple Configurator 2 können Geräte für die Aktivierung mit UEM vorbereitet werden. Benutzer können die vorbereiteten Geräte aktivieren, ohne den BlackBerry UEM Client 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 UEM-Domäne	VPP (Volume Purchase Program) ermöglicht Ihnen, iOS-Apps in Mengen zu kaufen und zu verteilen. Sie können Apple VPP-Konten mit einer UEM-Domäne verknüpfen, sodass Sie gekaufte Lizenzen für mit VPP-Konten verknüpfte iOS-Apps verteilen können.
Programm zur Geräteregistrierung (DEP) von Apple	Sie können UEM für die Verwendung des Programms zur Geräteregistrierung (DEP) von Apple konfigurieren, damit Sie UEM mit DEP synchronisieren können. Nach der Konfiguration von UEM können Sie die Aktivierung der von Ihrem Unternehmen für DEP erworbenen iOS-Geräte mit der Verwaltungskonsole verwalten. Sie können mehrere DEP-Konten verwenden. Sie können mehrere Apple-DEP-Konten mit einer UEM-Domäne verknüpfen.
Unterstützung für App-basierte PKI-Lösungen	UEM unterstützt 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.
Benutzerdefinierte Payload-Profile	Mit benutzerdefinierten Payload-Profilen können Sie Funktionen auf iOS-Geräten steuern, die nicht durch bestehende UEM-Richtlinien oder -Profile gesteuert werden. Sie können mit Apple ConfiguratorApple-Konfigurationsprofile erstellen und diese den benutzerdefinierten UEM-Payload-Profilen hinzufügen. Sie können benutzerdefinierte Payload-Profile Benutzern, Benutzergruppen und Gerätegruppen zuweisen.

Funktion	Beschreibung
BlackBerry Secure Gateway	BlackBerry Secure Gateway ermöglicht iOS-Geräten mit der Aktivierungsart „MDM-Steuerelemente“ die Verbindung zu einem geschäftlichen E-Mail-Server über die BlackBerry Infrastructure und UEM. Wenn Sie 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. Per App VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (bspw. 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“ 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.
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.

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 aktivieren.
IBM Notes Traveler-Unterstützung	iOS-Geräte können eine Verbindung zu IBM Notes Traveler über den BlackBerry Secure Gateway herstellen.
Face ID-Unterstützung	UEM unterstützt die Face ID für die Authentifizierung von Geräten und zum Öffnen von BlackBerry Dynamics-Apps.
Verwaltung freigegebener Geräte	Sie können zulassen, dass mehrere Benutzer ein iOS-Gerät gemeinsam verwenden. Sie können die Nutzungsbestimmungen anpassen, die Benutzer akzeptieren müssen, um freigegebene Geräte abzumelden. Ein Benutzer kann ein Gerät per lokaler Authentifizierung abmelden und sobald er fertig ist wieder anmelden, damit es für den nächsten Benutzer zur Verfügung steht. Freigegebene Geräte werden während des Abmeldungs- und Anmeldungsprozesses von UEM verwaltet. Diese Funktion wurde speziell für überwachte Geräte mit der folgenden Konfiguration entwickelt: • 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
Verwalten von Android Enterprise- und Android Management-Geräten	Sie können Android-Geräte für die Verwendung von Android Enterprise oder Android Management aktivieren. Diese Funktionen wurden von Google entwickelt und bieten zusätzliche Sicherheit für Unternehmen, die auf Android-Geräten Apps und Daten verwalten und zulassen wollen. Geräte können so aktiviert werden, dass sie nur ein geschäftliches oder sowohl ein geschäftliches als auch ein persönliches Profil haben. Sie haben die volle Kontrolle über beide Profile und können das gesamte Gerät löschen. Sie können dem Benutzer aber auch für das persönliche Profil Privatsphäre gewähren und sich nur für die geschäftlichen Daten auf dem Gerät Löschrechte vorbehalten. Samsung-Geräte bieten zusätzliche Administratoroptionen, unter anderem auch (bei einer Aktivierung mit Android Enterprise) erweiterte IT-Richtlinienregeln.

Funktion	Beschreibung
Aktivierungen für Android Enterprise- und Android Management-Geräte „Geschäftlich und persönlich – vollständige Kontrolle“	Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts. 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.
Verwalten von Geräten mit Knox MDM und Knox Workspace	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 Ihres Unternehmens und schützt letztere mithilfe erweiterter, von Samsung entwickelter Sicherheits- und Verwaltungsfunktionen. Wenn ein Gerät aktiviert wird, erkennt UEM automatisch, ob das Gerät Knox unterstützt. Zusätzlich zu den Standard-Verwaltungsfunktionen für Android bietet UEM die folgenden Funktionen 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.
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	UEM unterstützt Geräte, 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 Bereitstellung von Geräten. Die Zero-touch-Registrierung macht es IT-Administratoren einfach, Geräte online zu konfigurieren und ihre Verwaltung durchzusetzen, wenn Mitarbeiter ihre Geräte bekommen. Weitere Informationen zu Google finden Sie unter 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.
Unterstützung für App-basierte PKI-Lösungen	UEM unterstützt 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.
SafetyNet und Play Integrity	Wenn Administratoren Android SafetyNet- oder Google Play Integrity-Nachweise aktivieren, sendet 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-Geräte

Funktion	Beschreibung
Unterstützung für Windows 10-Geräte	Sie können Windows-Geräte – Windows 10-Mobilgeräte und Windows 10-Tablets und -Computer – verwalten.
Proxyunterstützung für Windows 10-Geräte	Sie können VPN- und geschäftliche Wi-Fi-Verbindungen für Windows 10-Geräte konfigurieren und einen Proxyserver als Teil des Wi-Fi-Profils für Windows 10 Mobile-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. Per App VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (bspw. 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.
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.
Zulassen von Virenschutzanbietern	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 zulässigen Anbieter aktiviert ist.
Entra ID-Einbindung	UEM unterstützt die Entra ID-Einbindung, um den MDM-Registrierungsvorgang für Windows 10-Geräte zu vereinfachen. Benutzer können Ihre Geräte bei UEM unter Zuhilfenahme ihres Entra ID-Benutzernamens und -Kennworts registrieren. Die Entra ID-Einbindung unterstützt außerdem Windows AutoPilot, sodass Windows 10-Geräte während der vorkonfigurierten Windows 10-Einrichtung automatisch mit UEM aktiviert werden können.

macOS-Geräte

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

Funktion	Beschreibung
Profile und Richtlinien	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). Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern. Benutzer aktivieren macOS-Geräte mithilfe von BlackBerry UEM Self-Service.

Unterstützte Leistungsmerkmale nach Gerätetyp

In dieser Kurzanleitung werden die unterstützten Funktionen von Geräten mit iOS, macOS, Android und Windows 10 in BlackBerry UEM verglichen.

Informationen zu den unterstützten Betriebssystemversionen finden Sie in der Konformitätsmatrix.

Gerätefunktionen

Funktion	iOS	macOS	Android	Windows 10
Drahtlose Aktivierung	√	√	√	√
Drahtlose Aktivierung mithilfe eines QR-Codes	√		√	
Client-App zur Aktivierung erforderlich	√ [1]		√	
Anpassen der Nutzungsbedingungen für die Aktivierung	√	√	√	√
Aktivierung nach Gerätemodell einschränken	√	√	√	
Gerätebericht anzeigen und exportieren (z. B. Details zur Hardware)	√	√	√	√
Einschränkungen für nicht überwachte Geräte	√[2]	√[2]		

[1] Bei iOS-Geräten, die in DEP angemeldet sind, muss die Client-App Benutzern oder Gruppen zugewiesen werden.

[2] Bei Geräten, die mit MDM-Steuerungen oder Privatsphäre des Benutzers mit SIM-basierter Lizenzierung aktiviert wurden.

Sicherheitsmerkmale

Funktion	iOS	macOS	Android	Windows 10
Trennung von geschäftlichen und persönlichen Daten	√ [1]		√ [2]	√
Benutzer-Datenschutz für persönliche Daten	√ [1]		√ [2]	
Verschlüsselung von geschäftlichen Daten im Ruhezustand	√ [1]		√ [2]	√
IT-Administrationsbefehle an Geräte senden	√	√	√	√
Steuern von Gerätefunktionen mithilfe von IT-Richtlinien	√	√	√	√
Geschäftliche Daten nach einem Zeitraum der Inaktivität löschen	√ [1]		√ [1]	
Durchsetzung von Kennwortanforderungen	√	√	√	√
Erzwingen der Verschlüsselung von Medienkarten			√ [3]	
Erzwingen der Verschlüsselung des internen Speichers			√	√

[1] Erfordert BlackBerry Dynamics-Apps.

[2] Erfordert Samsung Knox Workspace, Android Enterprise, Android Management oder BlackBerry Dynamics-Apps.

[3] Nur für Samsung Knox-Geräte.

Senden von Zertifikaten an Geräte

Funktion	iOS	macOS	Android	Windows 10
Profile für Zertifizierungsstellenzertifikate	√	√	√	√
SCEP-Profile	√	√	√	√
Profile für freigegebenes Zertifikat	√	√	√	
Profile für Benutzeranmelde-informationen	√	√	√	

Verwaltung von Geschäftsverbindungen für Geräte

Funktion	iOS	macOS	Android	Windows 10
BlackBerry 2FA-Profile	√		√	
BlackBerry Dynamics-Konnektivitätsprofile	√	√	√	√
CalDAV-Profile	√	√		
CardDAV-Profile	√	√		
Enterprise-Konnektivität				
BlackBerry Secure Connect Plus	√		√ [1]	
Exchange ActiveSync E-Mail-Profile	√	√	√ [2]	√
BlackBerry Secure Gateway	√			
IMAP/POP3 E-Mail-Profile	√	√	√	√
Proxy-Profile	√	√	√	√
Profile für die einmalige Anmeldung	√			
VPN-Profile	√	√	√ [3]	√
Wi-Fi-Profile	√	√	√	√

[1] Nur bei Android Enterprise-Geräten und Knox Workspace-Geräten.

[2] Nur bei Motorola-Geräten, die EDM-API unterstützen, Android Enterprise-Geräten und Knox-Geräten.

[3] Nur für Knox Workspace-Geräte.

Verwalten der Gerätestandards für Ihre Organisation

Funktion	iOS	macOS	Android	Windows 10
Aktivierungsprofile	√	√	√	√
Profile für App-Sperrmodus	√ [1]		√ [1]	√ [1]
BlackBerry Dynamics-Profile	√	√	√	√
Konformitätsprofile	√		√	
Geräteprofile	√		√	

Funktion	iOS	macOS	Android	Windows 10
Enterprise Management Agent-Profile	√		√	√
Profile für die Standortbestimmung	√		√	√

[1] Nur für überwachte iOS-Geräte, Knox-Geräte, die mit MDM-Steuerelemente aktiviert wurden, Windows 10 Education- und Windows 10 Enterprise-Geräte.

Schützen von verlorenen oder gestohlenen Geräten

Funktion	iOS	macOS	Android	Windows 10
Gerätekennwort festlegen			√	
Gerät sperren	√	√	√	
Aktivierungssperre	√			
Gerätekennwort festlegen und sperren			√	
Geschäftlichen Bereich sperren und Kennwort festlegen			√ [1]	
Gerät entsperren und Kennwort löschen	√		√	
Alle Gerätedaten löschen	√	√	√ [2]	√
Nur geschäftliche Daten löschen	√	√	√	√

[1] Nur bei Android Enterprise-Geräten.

[2] Bei Motorola-Geräten, die die EDM API unterstützen, werden die Informationen auf der Medienkarte ebenfalls gelöscht. Bei Geräten mit Knox Workspace können Sie optional ebenfalls die Daten auf der Medienkarte löschen.

Konfigurieren des Roaming

Funktion	iOS	macOS	Android	Windows 10
Deaktivieren der automatischen Synchronisierung beim Roaming	√		√ [1]	
Deaktivieren von Daten während des Roaming	√[2]		√ [3]	√

[1] Nur für Knox-Geräte.

[2] Sie können Einstellungen für das Daten-Roaming in einem Netzwerknutzungsprofil konfigurieren.

[3] Nur bei Android Enterprise- und Knox-Geräten.

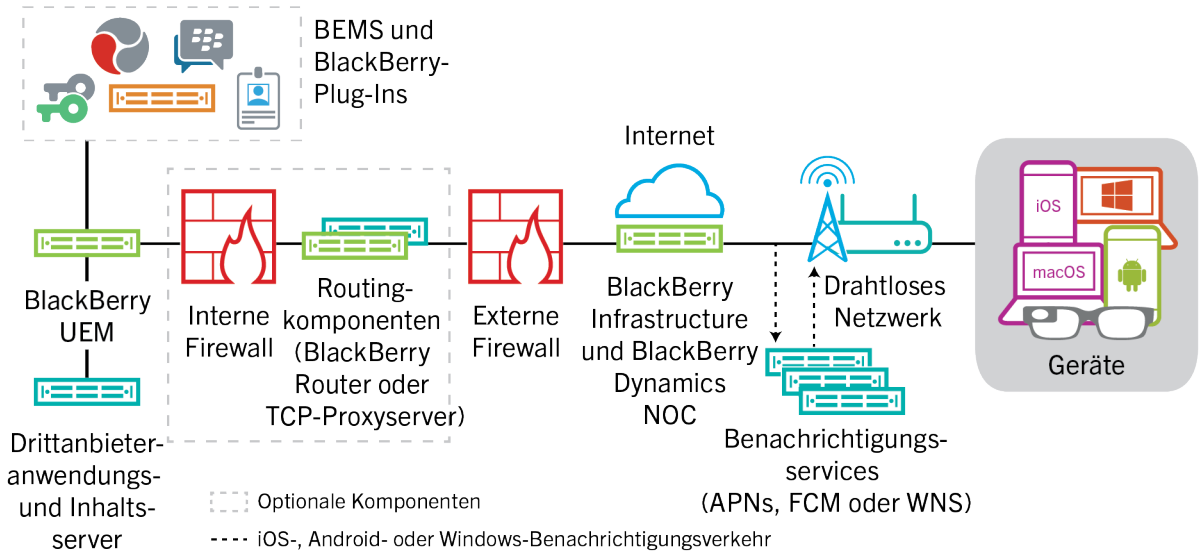
Verwalten von Apps

Funktion	iOS	macOS	Android	Windows 10
Verteilen von öffentlichen Apps von der Verkaufsplattform (App Store, Google Play, Windows Store, BlackBerry World)	√		√	√
Verwalten des Katalogs geschäftlicher Apps	√		√	√
Markenkatalog geschäftlicher Apps	√			
Apps sperren	√		√	
Verteilen interner Apps	√		√	√
App-Verknüpfungen zu Geräten hinzufügen	√	√	√	

BlackBerry UEM-Architektur

Die BlackBerry UEM-Architektur wurde entwickelt, um Sie bei der Verwaltung mobiler Geräte in Ihrem Unternehmen zu unterstützen und eine sichere Verbindung für Daten bereitzustellen, die zwischen E-Mail- und den Inhaltsservern sowie den Geräten der Benutzer übertragen werden.

Architektur: BlackBerry UEM-Lösung



Komponente	Beschreibung
BlackBerry UEM	BlackBerry UEM ist eine einheitliche Endpunktverwaltungslösung, die umfassende Funktionen für die plattformübergreifende Verwaltung von Geräten und Anwendungen sowie für das Content Management mit integrierter Sicherheit und Konnektivität bietet.
BlackBerry Infrastructure	Die BlackBerry Infrastructure ist ein globales privates Datennetzwerk, das über mehrere Regionen verteilt ist und die Datenübertragung zwischen Tausenden von Unternehmen und Millionen von Benutzern weltweit ermöglicht und sichert. Sie ist darauf ausgelegt, den Transport von Daten zwischen BlackBerry-Diensten und Endbenutzergeräten effizient zu verwalten. Für Unternehmen mit UEM registriert die BlackBerry Infrastructure Benutzerinformationen für die Geräteaktivierung, überprüft Lizenzinformationen und stellt einen vertrauenswürdigen Pfad, der auf einer starken, kryptografischen gegenseitigen Authentifizierung beruht, zwischen dem Unternehmen und jedem Benutzer bereit. UEM ermöglicht eine konstante Verbindung zur BlackBerry Infrastructure, sodass Unternehmen nur eine einzelne ausgehende Verbindung zu einer vertrauenswürdigen IP-Adresse benötigen, um Daten an Benutzer zu senden. Alle Daten zwischen der BlackBerry Infrastructure und UEM werden authentifiziert und verschlüsselt, um für Geräte außerhalb der Firewall einen sicheren Kommunikationskanal in Ihr Unternehmen bereitzustellen.

Komponente	Beschreibung
BlackBerry Dynamics NOC	Das BlackBerry Dynamics NOC ist ein Netzwerkbetriebszentrum, das eine sichere Kommunikation zwischen den BlackBerry Dynamics-Apps auf Geräten und UEM sowie dem BlackBerry Enterprise Mobility Server ermöglicht.
Geräte	BlackBerry UEM unterstützt Geräte mit iOS, macOS, Android und Windows.
Benachrichtigungsdienste	UEM sendet Benachrichtigungen an Geräte, um UEM wegen Updates zu kontaktieren und Informationen über den Gerätebestand Ihres Unternehmens zu übermitteln. Diese Benachrichtigungen werden an die BlackBerry Infrastructure gesendet, wo sie mithilfe des entsprechenden Benachrichtigungsdiensts an die Geräte gesendet werden. • APNs ist ein Apple-Dienst zum Senden von Benachrichtigungen an iOS- und macOS-Geräte. • FCM ist ein Google-Dienst zum Senden von Benachrichtigungen an Android-Geräte. • Windows-Pushbenachrichtungsdienst (WNS) ist ein Microsoft-Dienst zum Senden von Benachrichtigungen an Windows-Geräte.
Routingkomponenten	Standardmäßig stellt UEM über die Ports 3101 und 443 eine direkte Verbindung mit der BlackBerry Infrastructure her, sodass Sie keine weiteren Routingkomponenten installieren müssen. Wenn die Sicherheitsstandards Ihres Unternehmens jedoch vorschreiben, dass interne Systeme keine direkten Verbindungen mit dem Internet herstellen dürfen, können Sie den BlackBerry Router oder einen Proxyserver verwenden. Der BlackBerry Router agiert als Proxy-Server für Verbindungen über die BlackBerry Infrastructure zwischen UEM und allen Geräten. Der BlackBerry Router kann SOCKs v5 ohne Authentifizierung unterstützen. Wenn Ihr Unternehmen schon einen TCP-Proxy-Server installiert hat oder einen benötigt, um die Netzwerkanforderungen zu erfüllen, können Sie einen TCP-Proxy-Server anstelle des BlackBerry Router verwenden. Der TCP-Proxy-Server kann SOCKs v5 ohne Authentifizierung unterstützen. Der BlackBerry UEM Core und BlackBerry Proxy unterstützen das Herstellen von Verbindungen mit dem BlackBerry Dynamics NOC über einen HTTP-Proxyserver.
Drittanbieteranwendungs- und Inhaltsserver	Zusätzliche Inhaltsserver und Anwendungsserver in der Unternehmensumgebung, einschließlich Unternehmensverzeichnis, Mailserver, Zertifizierungsstellen usw.
BlackBerry-Plug-ins und BEMS	UEM ist mit zusätzlichen BlackBerry-Unternehmensprodukten, z. B. BlackBerry Enterprise Identity, BlackBerry 2FA und BlackBerry Workspaces kompatibel, um die UEM-Funktionen in Ihrem Unternehmen zu erweitern. Weitere Informationen finden Sie unter Zugehörige Produkte und Dienste. Der BlackBerry Enterprise Mobility Server stellt Dienste bereit, die zum Übertragen von geschäftlichen Daten zwischen BlackBerry Dynamics-Apps verwendet werden. Weitere Informationen finden Sie in der Dokumentation für BlackBerry Enterprise Mobility Server.

Architektur: BlackBerry UEM Cloud-Lösung

Die BlackBerry UEM Cloud-Architektur wurde entwickelt, um Sie bei der Verwaltung mobiler Geräte für Ihr Unternehmen in einer Cloud-Umgebung zu unterstützen und eine sichere Verbindung für Daten bereitzustellen, die zwischen E-Mail- und Inhaltsservern und den Geräten der Benutzer übertragen werden.

Komponente	Beschreibung
BlackBerry UEM Cloud	BlackBerry UEM Cloud ist ein Dienst für die Verwaltung von Geräten, die in der Umgebung Ihres Unternehmens verwendet werden.
BlackBerry Infrastructure und BlackBerry Dynamics NOC	Die BlackBerry Infrastructure registriert Benutzerinformationen für die Geräteaktivierung und überprüft Lizenzinformationen. Wenn Sie BlackBerry Secure Connect Plus oder BlackBerry Secure Gateway aktivieren, werden Daten, die diese Dienste verwenden, bei der Übertragung über die BlackBerry Infrastructure geleitet. BlackBerry Dynamics NOC ist ein separates Netzbetriebszentrum (Network Operation Center, NOC), das eine sichere Kommunikation zwischen BlackBerry Dynamics-Apps auf Geräten und BlackBerry Proxy hinter der Firewall als Teil des BlackBerry Connectivity Node bietet.
Geräte	BlackBerry UEM Cloud unterstützt Geräte mit iOS, macOS, Android und Windows.
Benachrichtigungsdienste	UEM Cloud sendet Benachrichtigungen an Geräte, um mögliche Updates von UEM abzurufen und Informationen über den Gerätebestand Ihres Unternehmens zu übermitteln. Diese Benachrichtigungen werden an die BlackBerry Infrastructure gesendet, wo sie mithilfe des entsprechenden Benachrichtigungsdiensts an die Geräte gesendet werden: • APNs ist ein Apple-Dienst zum Senden von Benachrichtigungen an iOS- und macOS-Geräte. • FCM ist ein Google-Dienst zum Senden von Benachrichtigungen an Android-Geräte. • WNS ist ein Microsoft-Dienst zum Senden von Benachrichtigungen an Windows 10-Geräte.

Komponente	Beschreibung
BlackBerry Connectivity Node	Der BlackBerry Connectivity Node ist eine optionale Komponente, die Sie innerhalb der Firewall Ihres Unternehmens installieren. Er enthält fünf Komponenten, die UEM Cloud um weitere Funktionen erweitern: • Der BlackBerry Cloud Connector stellt eine Verbindung zwischen Ihrem Unternehmensverzeichnis und UEM Cloud hinter der Firewall Ihres Unternehmens her, um die Synchronisierung von Attributen, eine Suchfunktion und Dienste zur Authentifizierung von Benutzern zuzulassen. Wenn Sie den BlackBerry Connectivity Node nicht installieren und sich Ihr Unternehmensverzeichnis hinter der Firewall befindet, müssen Sie lokale Benutzerkonten in UEM Cloud erstellen, anstatt die in Ihrem Unternehmensverzeichnis aufgeführten Benutzerkonten zu verwenden. Der BlackBerry Cloud Connector ist nicht erforderlich, damit UEM Cloud eine Verbindung zu Microsoft Entra ID herstellt. • BlackBerry Proxy hält eine sichere Verbindung zwischen Ihrem Unternehmen und BlackBerry Dynamics NOC aufrecht, die BlackBerry Dynamics-Apps eine sichere Kommunikation mit den Ressourcen Ihres Unternehmens hinter der Firewall erlaubt. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen von BlackBerry Dynamics NOC ermöglicht. • Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf UEM Cloud aktiviert werden. Nicht verwaltete Geräte, die versuchen, sich mit einem E-Mail-Server des Unternehmens zu verbinden, können durch einen Administrator über die UEM-Verwaltungskonsole überprüft, verifiziert und blockiert oder zugelassen werden. • BlackBerry Secure Connect Plus stellt einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf Geräten und dem Netzwerk des Unternehmens her. Ein Tunnel, der standardmäßige IPV4-Daten (TCP und UDP) unterstützt, wird für jedes Gerät über die BlackBerry Infrastructure bereitgestellt. • BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und UEM Cloud zum E-Mail-Server Ihres Unternehmens für iOS-Geräte.
Unternehmensverzeichnis	UEM Cloud unterstützt Verbindungen zum Microsoft Active Directory Ihres Unternehmens bzw. zum LDAP-Unternehmensverzeichnis hinter der Firewall über den BlackBerry Connectivity Node.
Microsoft Entra ID (ehemals Azure AD)	Microsoft Entra ID ist ein Cloud-basierter Verzeichnisverwaltungsdienst. Wenn Ihr Unternehmen Entra ID verwendet, können Sie eine Verbindung dazu anstatt oder zusätzlich zum Unternehmensverzeichnis hinter der Firewall herstellen.

Komponente	Beschreibung
Inhalts-, Anwendungs- und Mail-Server	Wenn Sie BlackBerry Secure Connect Plus aktivieren, oder wenn Benutzer BlackBerry Dynamics-Apps haben, können Geräte eine Verbindung mit den Servern Ihres Unternehmens herstellen, ohne dass Sie eine direkte Verbindung zwischen dem Server und dem Internet herstellen müssen. Geschäftliche Daten während der Übertragung zwischen Ihren Servern und Geräten werden über BlackBerry Secure Connect Plus und BlackBerry Infrastructure gesendet. BlackBerry Dynamics-App-Daten werden über BlackBerry Proxy und BlackBerry Dynamics NOC gesendet. BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und BlackBerry Connectivity Node zwischen dem E-Mail-Server Ihres Unternehmens und iOS-Geräten.
BlackBerry-Plug-ins und BEMS	UEM ist mit zusätzlichen BlackBerry-Unternehmensprodukten, z. B. BlackBerry Enterprise Identity, BlackBerry 2FA und BlackBerry Workspaces kompatibel, um die UEM-Funktionen in Ihrem Unternehmen zu erweitern. Weitere Informationen finden Sie unter Zugehörige Produkte und Dienste. Der BlackBerry Enterprise Mobility Server stellt Dienste bereit, die zum Übertragen von geschäftlichen Daten zwischen BlackBerry Dynamics-Apps verwendet werden. Weitere Informationen finden Sie in der Dokumentation für BlackBerry Enterprise Mobility Server.

Lokale BlackBerry UEM-Komponenten

Dieses Diagramm zeigt, wie die BlackBerry UEM-Komponenten miteinander verbunden sind, wenn alle Komponenten in der einfachsten Konfiguration des Produkts gemeinsam installiert werden.

Komponentenname	Beschreibung
BlackBerry UEM Core	BlackBerry UEM Core ist die zentrale Komponente der UEM-Architektur. Er weist mehrere Unterkomponenten auf, die verantwortlich sind für: • Protokollierung, Überwachung, Reporting und Verwaltungsfunktionen • Authentifizierungs- und Autorisierungsdienste • Planen und Senden von Befehlen, IT-Richtlinien und Profilen an Geräte • Sendet Benutzer-, Richtlinien- und andere Konfigurationsdaten an die BlackBerry Dynamics-Apps.
BlackBerry Proxy	Der BlackBerry Proxy sorgt für eine sichere Verbindung zwischen Ihrem Unternehmen und dem BlackBerry Dynamics NOC. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen des BlackBerry Dynamics NOC ermöglicht.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus stellt einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf Geräten und dem Netzwerk des Unternehmens her. Ein Tunnel, der standardmäßige IPV4-Daten (TCP und UDP) unterstützt, wird für jedes Gerät über die BlackBerry Infrastructure bereitgestellt.
BlackBerry Secure Gateway	Der BlackBerry Secure Gateway bietet eine sichere Verbindung über die BlackBerry Infrastructure und UEM zum E-Mail-Server Ihres Unternehmens für iOS-Geräte.
BlackBerry Gatekeeping Service	Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf UEM aktiviert werden. Nicht verwaltete Geräte, die versuchen, sich mit einem E-Mail-Server des Unternehmens zu verbinden, können durch einen Administrator über die Verwaltungskonsole überprüft, verifiziert und blockiert oder zugelassen werden.
Verwaltungskonsole und BlackBerry UEM Self-Service	Die Verwaltungskonsole und der BlackBerry UEM Self-Service bilden eine webbasierte Benutzerschnittstelle, die Administrator- und Benutzerzugriff auf UEM ermöglicht. Sie können Systemeinstellungen, Benutzer, Geräte und Apps über die Verwaltungskonsole verwalten. Benutzer können den UEM Self-Service verwenden, um ein Aktivierungskennwort einzurichten und Befehle, z. B. zum Einrichten des Kennworts, Sperren des Geräts und Löschen von Gerätedaten, an Geräte zu senden.
BlackBerry UEM-Datenbank	Die UEM-Datenbank ist eine relationale Datenbank, die Informationen zum Benutzerkonto und der Konfiguration enthält, die von UEM für die Verwaltung von Geräten und BlackBerry Dynamics-Apps verwendet werden.

Komponentenname	Beschreibung
BlackBerry Enterprise Mobility Server	Der BEMS führt verschiedene Dienste zusammen, die zum Übertragen von geschäftlichen Daten zwischen BlackBerry Dynamics-Apps verwendet werden, z. B.: • BlackBerry Push Notifications: Akzeptiert Push-Registrierungsanforderungen von iOS- und Android-Geräten und kommuniziert mit Microsoft Exchange, um das geschäftliche E-Mail-Konto des Benutzers auf Änderungen zu überwachen. • BlackBerry Connect: Ermöglicht sicheres Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen auf iOS- und Android-Geräten. • BlackBerry Presence: Stellt Informationen zum Anwesenheitsstatus für BlackBerry Dynamics-Apps in Echtzeit bereit. • BlackBerry Docs: Ermöglicht den Benutzern der BlackBerry Dynamics-App den Zugriff, die Synchronisierung und die gemeinsame Nutzung von Dokumenten über ihren geschäftlichen Dateiserver, SharePoint, Box und Content-Management-Systeme mit CMIS-Unterstützung, ohne Einsatz von VPN-Software, ohne Firewall-Neukonfiguration oder doppelte Datenspeicher. In den BEMS-Datenbanken werden Benutzer-, App-, Richtlinien- und Konfigurationsinformationen gespeichert.
BlackBerry Router und/oder Proxyserver	Standardmäßig stellt UEM eine direkte Verbindung mit der BlackBerry Infrastructure über die Ports 3101 und 443 her. Wenn die Sicherheitsstandards Ihres Unternehmens jedoch vorschreiben, dass interne Systeme keine direkten Verbindungen mit dem Internet herstellen dürfen, können Sie den BlackBerry Router oder einen TCP-Proxyserver eines Drittanbieters installieren, der SOCKs v5 ohne Authentifizierung unterstützt. Der UEM Core und BlackBerry Proxy unterstützen das Herstellen von Verbindungen mit dem BlackBerry Dynamics NOC über den HTTP-Proxyserver eines Drittanbieters.
BlackBerry Infrastructure und BlackBerry Dynamics NOC	Die BlackBerry Infrastructure registriert Benutzerinformationen für die Geräteaktivierung, überprüft Lizenzinformationen und stellt einen vertrauenswürdigen Pfad, der auf einer starken, kryptografischen gegenseitigen Authentifizierung basiert, zwischen dem Unternehmen und jedem Benutzer bereit. Das BlackBerry Dynamics NOC ist ein räumlich getrenntes NOC, das eine sichere Kommunikation zwischen den BlackBerry Dynamics-Apps auf Geräten und den UEM Core, BlackBerry Proxy sowie BEMS ermöglicht.

Lokale verteilte BlackBerry UEM-Installation

Dieses Diagramm zeigt, wie die BlackBerry UEM-Komponenten miteinander verbunden sind, wenn der BlackBerry Connectivity Node und die Benutzerschnittstelle getrennt von den primären UEM-Komponenten installiert werden.

Komponentenname	Beschreibung
Primäre UEM-Komponenten	Die primären UEM-Komponenten beinhalten den BlackBerry UEM Core und alle Komponenten, die mit ihm auf demselben Server installiert werden.
BlackBerry UEM Core	UEM Core ist die zentrale Komponente der UEM-Architektur. Er weist mehrere Unterkomponenten auf, die verantwortlich sind für: • Protokollierung, Überwachung, Reporting und Verwaltungsfunktionen • Authentifizierungs- und Autorisierungsdienste • Planen und Senden von Befehlen, IT-Richtlinien und Profilen an Geräte • Sendet Benutzer-, Richtlinien- und andere Konfigurationsdaten an die auf Geräten installierten BlackBerry Dynamics-Apps.
BlackBerry UEM-Datenbank	Die UEM-Datenbank ist eine relationale Datenbank, die Informationen zum Benutzerkonto und der Konfiguration enthält, die von UEM für die Verwaltung von Geräten und BlackBerry Dynamics-Apps verwendet werden.
BlackBerry Gatekeeping Service (primär)	Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf UEM aktiviert werden. Nicht verwaltete Geräte, die versuchen, sich mit einem E-Mail-Server des Unternehmens zu verbinden, können über die Verwaltungskonsole überprüft, verifiziert und blockiert oder zugelassen werden.
Remote-UI-Komponenten	Die Verwaltungskonsole und BlackBerry UEM Self-Service können separat von anderen UEM-Komponenten installiert werden. Wenn Sie sie separat installieren, wird auch eine BlackBerry Management Console Core-Instanz installiert.
BlackBerry Management Console Core	Falls installiert, verarbeitet die BlackBerry Management Console Core nur UI-Anforderungen von der Verwaltungskonsole und von UEM Self-Service. Dadurch wird sichergestellt, dass diese Schnittstellen auch bei einer hohen Belastung von UEM Core reagieren.
Verwaltungskonsole und BlackBerry UEM Self-Service	Die Verwaltungskonsole und der UEM Self-Service bilden eine webbasierte Benutzerschnittstelle, die Administrator- und Benutzerzugriff auf UEM ermöglicht. Sie können separat von anderen Komponenten installiert werden. Sie können Systemeinstellungen, Benutzer, Geräte und Apps über die Verwaltungskonsole verwalten. Benutzer können auf denUEM Self-Service zugreifen, um ein Aktivierungskennwort einzurichten und Befehle, z. B. zum Einrichten des Kennworts, Sperren des Geräts und Löschen von Gerätedaten, an Geräte zu senden.

Komponentenname	Beschreibung
BlackBerry Connectivity Node	Der BlackBerry Connectivity Node installiert Instanzen der UEM-Geräteverbindungskomponenten, die eine Verbindung mit der Domäne Ihres Unternehmens herstellen, auf einem anderen Server als der UEM Core. Jeder BlackBerry Connectivity Node beinhaltet die folgenden Komponenten: • BlackBerry Cloud Connector: Ermöglicht die Kommunikation der BlackBerry Connectivity Node-Komponenten mit dem UEM Core. Die Kommunikation zwischen dem BlackBerry Cloud Connector und UEM Core erfolgt über die BlackBerry Infrastructure. • BlackBerry Proxy: Sorgt für eine sichere Verbindung zwischen Ihrem Unternehmen und dem BlackBerry Dynamics NOC. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen des BlackBerry Dynamics NOC ermöglicht. • BlackBerry Secure Connect Plus: Stellt einen sicheren IP-Tunnel zwischen Apps für den geschäftlichen Bereich auf Geräten und dem Netzwerk des Unternehmens her. Ein Tunnel, der standardmäßige IPV4-Daten (TCP und UDP) unterstützt, wird für jedes Gerät über die BlackBerry Infrastructure bereitgestellt. • BlackBerry Secure Gateway: Bietet eine sichere Verbindung über die BlackBerry Infrastructure und UEM zum E-Mail-Server Ihres Unternehmens für iOS-Geräte. • BlackBerry Gatekeeping Service: Gatekeeping für Ihren E-Mail-Server verwalten. Wenn Gatekeeping-Daten nur von dem BlackBerry Gatekeeping Service verwaltet werden sollen, der mit den primären UEM-Komponenten installiert ist, können Sie die BlackBerry Gatekeeping Service in jedem BlackBerry Connectivity Node deaktivieren.
BlackBerry Enterprise Mobility Server	Der BEMS führt verschiedene Dienste zusammen, die zum Übertragen von geschäftlichen Daten zwischen BlackBerry Dynamics-Apps verwendet werden, z. B.: • BlackBerry Push Notifications: Akzeptiert Push-Registrierungsanforderungen von iOS- und Android-Geräten und kommuniziert mit Microsoft Exchange, um das geschäftliche E-Mail-Konto des Benutzers auf Änderungen zu überwachen. • BlackBerry Connect: Ermöglicht sicheres Instant Messaging, Suchanfragen im Unternehmensverzeichnis und Anwesenheitsbenachrichtigungen auf iOS- und Android-Geräten. • BlackBerry Presence: Stellt Informationen zum Anwesenheitsstatus für BlackBerry Dynamics-Apps in Echtzeit bereit. • BlackBerry Docs: Ermöglicht den Benutzern der BlackBerry Dynamics-App den Zugriff, die Synchronisierung und die gemeinsame Nutzung von Dokumenten über ihren geschäftlichen Dateiserver, SharePoint, Box und Content-Management-Systeme mit CMIS-Unterstützung, ohne Einsatz von VPN-Software, ohne Firewall-Neukonfiguration oder doppelte Datenspeicher. In den BEMS-Datenbanken werden Benutzer-, App-, Richtlinien- und Konfigurationsinformationen gespeichert.

Komponentenname	Beschreibung
BlackBerry Infrastructure und BlackBerry Dynamics NOC	Die BlackBerry Infrastructure registriert Benutzerinformationen für die Geräteaktivierung, überprüft Lizenzinformationen und stellt einen vertrauenswürdigen Pfad, der auf einer starken, kryptografischen gegenseitigen Authentifizierung basiert, zwischen dem Unternehmen und jedem Benutzer bereit. Das BlackBerry Dynamics NOC ist ein räumlich getrenntes NOC, das eine sichere Kommunikation zwischen den BlackBerry Dynamics-Apps auf Geräten und den UEM Core, BlackBerry Proxy sowie BEMS ermöglicht.

Zugehörige Produkte und Dienste

Dieser Abschnitt enthält Informationen über die vielen Begleitprodukte und -Dienste, die mit BlackBerry UEM verwendet werden können.

Enterprise- und BlackBerry Dynamics-Apps

BlackBerry Enterprise-Apps

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	Der BlackBerry UEM Client gestattet UEM die Verwaltung von iOS- und Android-Geräten. Benutzer benötigen UEM Client, wenn sie iOS- oder Android-Geräte für die Verwaltung mobiler Geräte mit UEM aktivieren möchten. Benutzer können die neueste Version des UEM Client von App Store oder Google Play herunterladen. Nachdem Benutzer ihre Geräte aktiviert haben, bietet der UEM Client folgende Möglichkeiten: • Überprüfung der Konformität ihrer Geräte mit den Standards des Unternehmens • Ansicht der Profile, die ihnen zugewiesen sind • Ansicht der IT-Richtlinienregeln, die ihnen 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 Weitere Informationen finden Sie in der Dokumentation zu UEM Client.
BBM Enterprise	BBM Enterprise fügt eine zusätzliche Schicht für die durchgehende Verschlüsselung von BBM-Nachrichten hinzu, die zwischen BBM Enterprise-Benutzern in Ihrem Unternehmen und anderen BBM-Benutzern innerhalb und außerhalb Ihres Unternehmens ausgetauscht werden. BBM Enterprise ist für iOS-, Android-, Windows- und macOS-Geräte verfügbar. 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. Bei den meisten Geräten können Sie UEM Benutzern mithilfe von BBM Enterprise zuweisen. Nach der Aktivierung der Benutzer für die Verwendung von BBM Enterprise können Benutzer die App im entsprechenden App Store herunterladen. Weitere Informationen finden Sie in der Dokumentation zu BBM Enterprise.

BlackBerry Dynamics-Apps

Die Produktivitäts-Apps von BlackBerry Dynamics ermöglichen Benutzern den Zugriff auf geschäftliche Daten und Produktivitäts-Tools.

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

Ihr Unternehmen kann auch benutzerdefinierte BlackBerry Dynamics-Apps mit dem BlackBerry Dynamics SDK entwickeln. Weitere Informationen finden Sie in der Dokumentation zu BlackBerry Dynamics SDK.

Vorteile von BlackBerry Enterprise Identity

BlackBerry Enterprise Identity erleichtert Benutzern den Zugriff auf Cloud-Anwendungen von jedem Gerät aus, z. B. von iOS, Android und 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, Google Workspace, 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 UEM-Verwaltungskonsole Dienste hinzufügen, Benutzer verwalten und weitere Administratoren hinzufügen und verwalten. Die Integration in UEM vereinfacht die Verwaltung von Benutzern und gewährt ihnen Zugriff auf Cloud-Anwendungen und -Dienste über ihre Geräte. Cloud-Dienste und die Binärdateien mobiler Apps können gebündelt und dann auf einfache Weise Benutzern oder Gruppen zugewiesen werden.

Weitere Informationen 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. Sie können ihre iOS- und Android-Geräte als zweiten Faktor für die Authentifizierung über eine einfache Bestätigungsaufforderung verwenden, wenn Benutzer versuchen, eine Verbindung zu den Ressourcen Ihres Unternehmens herzustellen.

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 UEM-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 finden Sie in der Dokumentation zu BlackBerry 2FA.

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 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 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 UEM-Verwaltungskonsole zu integrieren.

Falls Ihr Unternehmen auch BlackBerry Enterprise Identity implementiert hat, können Sie Enterprise Identity zur Verwaltung der Benutzerberechtigung für Workspaces verwenden.

Weitere Informationen finden Sie in der Dokumentation zu BlackBerry Workspaces.

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 finden Sie in der Dokumentation zu UEM Notifications.

BlackBerry-Unternehmens-SDKs

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

SDK	Beschreibung
BlackBerry Dynamics SDK	Das BlackBerry Dynamics SDK bietet leistungsstarke Tools, mit denen Entwickler sich auf die Erstellung nützlicher Produktivitätsanwendungen konzentrieren können, anstatt zu lernen, wie diese Apps gesichert, bereitgestellt und verwaltet werden. Entwickler können mit dem BlackBerry Dynamics SDK Apps für alle wichtigen Plattformen entwickeln, die wertvolle Dienste nutzen, einschließlich sicherer Kommunikation, Datenaustausch zwischen Anwendungen, Präsenz, Push, Verzeichnissuche, Single Sign-On-Authentifizierung sowie Identitäts- und Zugriffsmanagement. Weitere Informationen finden Sie in der Dokumentation zu BlackBerry Dynamics SDK.

SDK	Beschreibung
BlackBerry Web Services	Bei den BlackBerry Web Services handelt es sich um eine Sammlung von SOAP- und REST-Webdiensten, mit denen Entwickler Anwendungen zur Verwaltung der 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. Weitere Informationen finden Sie in der Dokumentation zu BlackBerry Web Services.
BlackBerry Workspaces Android-SDK	Entwickler können das BlackBerry Workspaces Android SDK verwenden, um Apps zu entwickeln, damit Benutzer mit Dateien arbeiten können, die durch BlackBerry Workspaces geschützt sind. Weitere Informationen finden Sie in der Dokumentation zum BlackBerry Workspaces Android SDK.

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

Rechtliche Hinweise

Patente, sofern zutreffend, zu finden unter: www.blackberry.com/patents.

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada