BlackBerry UEM

Verwalten von iOS-Geräten

12.17

Contents

Verwaltung von iOS- und iPadOS-Geräten

BlackBerry UEM ermöglicht eine präzise Verwaltung der Verbindung von iOS- und iPadOS-Geräten mit dem Netzwerk, der aktivierten Funktionen und der verfügbaren Apps. Unabhängig davon, ob Ihre Geräte Eigentum Ihres Unternehmens oder Ihrer Benutzer sind, können Sie mobilen Zugriff auf die Informationen Ihres Unternehmens gewähren und diese gleichzeitig vor allen Personen schützen, die keinen Zugriff haben sollten.

Apple hat iPadOS als eigenständiges Betriebssystem eingeführt, das mit iPadOS Version 13 startet. Aufgrund der umfangreichen Ähnlichkeiten zwischen iOS und iPadOS gelten fast alle BlackBerry UEM-Funktionen und Dokumentationen, die für iOS gelten, auch für iPadOS.

In diesem Handbuch wird erläutert, welche Optionen Sie zur Verwaltung von iOS- und iPadOS-Geräten haben und wie Sie die verfügbaren Funktionen im Einzelnen nutzen können.

Verwalten anderer Apple-Geräte

Sie können in BlackBerry UEM auch macOS- und Apple TV-Geräte aktivieren und verwalten. Apple TV ist ein digitaler Media-Player, der Daten empfangen und über ein HDMI-Kabel auf ein Fernsehgerät streamen kann.

BlackBerry UEM unterstützt die Apple TV Versionen der zweiten Generation oder höher. Weitere Informationen zu den unterstützten macOS Versionen finden Sie in der Kompatibilitätsmatrix. Zum Verwalten von Apple TV-Geräten befolgen Sie die Anweisungen, und verwenden Sie die Profileinstellungen für iOS-Geräte. Die folgenden BlackBerry UEM-Funktionen werden für Apple TV unterstützt:

- Geräteaktivierung mit BlackBerry UEM Self-Service
- Aktivierung mit MDM-Steuerelementen
- Wi-Fi und Zertifikatprofile
- Profile für App-Sperrmodus
- Gerätebefehle

Um zu verhindern, dass Benutzer Apple TV aktivieren, setzen Sie die Gerätemodell-Einschränkungen im Aktivierungsprofil so fest, dass keine Apple TV-Geräte zulässig sind. Weitere Informationen zum Aktivieren von macOS- und Apple TV-Geräten finden Sie in der Dokumentation zur Geräteaktivierung.

Was Sie auf iOS-Geräten steuern können

BlackBerry UEM bietet alle Tools, die Sie zur Steuerung der Funktionen benötigen, die mit iOS- und iPadOS-Geräten verwaltet werden können. Darüber hinaus bietet es Funktionen, mit denen Sie Gerätebenutzern einen sicheren Zugriff auf geschäftliche Ressourcen gewähren können, ohne das Gerät vollständig verwalten zu müssen.

Steuerungsebene	Beschreibung
Nicht verwaltete und teilweise verwaltete Geräte (Geräte, die auf BlackBerry UEM aktiviert, aber nicht vollständig verwaltet sind)	Sie können ein Gerät auf BlackBerry UEM aktivieren, um einen sicheren Zugriff auf geschäftliche Ressourcen zu ermöglichen, ohne das Gerät vollständig zu verwalten. Diese Option wird häufig für BYOD-Geräte verwendet. Diese Aktivierungen ermöglichen es Benutzern, über VPN mithilfe von BlackBerry 2FA auf Ihr Netzwerk zuzugreifen, Dateien sicher mithilfe von BlackBerry Workspaces freizugeben und BlackBerry Dynamics-Apps wie BlackBerry Work und BlackBerry Access zu installieren, um auf geschäftliche E-Mails und Ihr geschäftliches Intranet zuzugreifen.
Teilweise verwaltete Geräte mit einem geschäftlichen Profil	Sie können ein Gerät auf BlackBerry UEM aktivieren, um einen sicheren Zugriff auf geschäftliche Ressourcen in einem geschäftlichen Profil zu ermöglichen. Diese Option wird häufig für BYOD-Geräte verwendet. Bei dieser Aktivierungsart wird ein separater geschäftlicher Bereich auf dem Gerät für geschäftliche Apps und native Notizen, iCloud Drive, E-Mails (Anhänge und vollständige E-Mail-Texte), Kalender (Anhänge) und iCloud Keychain-Apps installiert.
Verwaltete Geräte (Geräte, die von BlackBerry UEM verwaltet werden)	Sie können ein Gerät aktivieren, um es vollständig von BlackBerry UEM zu verwalten. Diese Option wird häufig für unternehmenseigene Geräte verwendet. Diese Option ermöglicht die Verwaltung von geschäftlichen Daten über Befehle und IT-Richtlinienregeln. Sie können geschäftliche Apps, wie z. B. BlackBerry Dynamics-Apps, auf dem Gerät verwalten. BlackBerry UEM unterstützt die Verwaltung von iOS-Geräten unter Aufsicht. Einige IT-Richtlinienregeln werden nur auf Geräten unter Aufsicht unterstützt.

Benutzerdatenschutzaktivierungen können begrenzte Geräteverwaltungsfunktionen bieten und Benutzern den Zugriff auf geschäftliche Daten über BlackBerry Dynamics-Apps wie BlackBerry Work und BlackBerry Access ermöglichen. Sie können einige der folgenden Geräteverwaltungsfunktionen zulassen:

- Zugriff auf Informationen zur SIM-Karte und Gerätehardware: Zugriff auf SIM-Karten- und Hardwareinformationen durch BlackBerry UEM zulassen, um die SIM-basierte Lizenzierung zu aktivieren.
- App-Verwaltung: Zulassen, dass Administratoren geschäftliche Apps installieren oder löschen können und eine Liste der installierten geschäftlichen Apps auf dem Bildschirm mit den Benutzerdetails angezeigt wird.
- IT-Richtlinienverwaltung: Zulassen, dass ein begrenzter Satz von IT-Richtlinienregeln auf das Gerät angewendet wird (Kennwortrichtlinien, Screenshots zulassen, Dokumente aus verwalteten Quellen in nicht verwalteten Zielen zulassen und Dokumente aus nicht verwalteten Quellen in verwalteten Zielen zulassen).
- E-Mail-Profilverwaltung: Zulassen, dass E-Mail-Profile auf das Gerät angewendet werden.
- Wi-Fi-Profilverwaltung: Zulassen, dass Wi-Fi-Profile auf das Gerät angewendet werden.
- VPN-Profilverwaltung: Zulassen, dass VPN-Profile auf das Gerät angewendet werden.

Mit der Aktivierungsart **Benutzerdatenschutz – Benutzerregistrierung** bleiben die Benutzerdaten privat und von den geschäftlichen Daten getrennt. Bei dieser Aktivierungsart wird ein separater geschäftlicher Bereich

für geschäftliche Apps und einige native Apps auf dem Gerät installiert. Diese Aktivierungsart ermöglicht die Verwendung von App-Verwaltung, IT-Richtlinienverwaltung, E-Mail-Profilen Wi-Fi-Profilen und „VPN pro App“. Administratoren können geschäftliche Daten verwalten (z. B. geschäftliche Daten löschen), ohne dass Auswirkungen auf persönliche Daten erfolgen.

Diese Aktivierungsart wird auf nicht überwachten Geräten mit iOS oder iPadOS OS 13.1 und höher unterstützt.

MDM-Steuerelemente-Aktivierungen bieten vollständige Unterstützung für die Verwaltung von iOS-Geräten, einschließlich der folgenden Funktionen:

- Durchsetzung von Kennwortanforderungen
- Steuerung von Gerätefunktionen mithilfe von IT-Richtlinien (z. B. Deaktivierung der Kamera oder Bluetooth)
- Erzwingung von Kompatibilitätsregeln
- Wi-Fi- und VPN-Verbindungsprofile (mit Proxy)
- Synchronisation von E-Mail, Kontakten und Kalender mit Geräten
- Versenden von Zertifizierungsstellen- und Clientzertifikaten an Geräte, um Authentifizierung und S/MIME zu ermöglichen
- Verwalten erforderlicher und zugelassener öffentlicher und interner Apps, einschließlich BlackBerry Dynamics-Apps
- Volle Unterstützung für Apple-DEP und -VPP
- Ortung und Schutz verlorener oder gestohlener Geräte

Hinweis: Einige Funktionen und BlackBerry Dynamics-Apps sind nicht für alle Lizenzstufen verfügbar. Weitere Informationen zu den verfügbaren Lizenzen finden Sie in der Dokumentation zur Lizenzierung.

Schritte zum Verwalten von iOS-Geräten

Schritt	Aktion
1	Installieren und konfigurieren Sie BlackBerry UEM gemäß den Installationsanweisungen für lokale Umgebungen oder den UEM Cloud -Konfigurationsanweisungen. Um iOS- und iPadOS-Geräte verwalten zu können, müssen Sie ein APNs-Zertifikat von Apple abrufen.
2	Wenn Ihr Unternehmen das Apple-Programm zur Geräteregistrierung verwendet, konfigurieren Sie BlackBerry UEM für die Verwendung von DEP.
3	Konfigurieren Sie die IT-Richtlinien für die Geräte. Weisen Sie Benutzergruppen oder einzelnen Benutzern IT-Richtlinien zu.
4	Konfigurieren Sie Profile für die Geräte. Weisen Sie Benutzergruppen oder einzelnen Benutzern Profile zu.
5	Wenn Ihr Unternehmen über ein Apple VPP-Konto verfügt, fügen Sie es zu BlackBerry UEM hinzu.
6	Geben Sie die Apps an, die Geräte installieren können oder müssen.
7	Aktivieren Sie Geräte.
8	Verwalten und überwachen Sie Geräte.

Steuerung von Geräten mit einer IT-Richtlinie

BlackBerry UEM sendet eine IT-Richtlinie an jedes Gerät. Sie können eine Standard-IT-Richtlinie verwenden oder eigene IT-Richtlinien erstellen. Sie können so viele IT-Richtlinien erstellen, wie Sie für verschiedene Situationen und Benutzer benötigen, aber auf einem Gerät ist immer nur eine IT-Richtlinie aktiv.

Die IT-Richtlinienregeln für iOS und iPadOS basieren auf den Funktionen des Geräts und den von Apple bereitgestellten Gerätekonfigurationsoptionen. Wenn Apple neue Betriebssystem-Updates mit neuen Funktionen und Konfigurationsoptionen veröffentlicht, werden UEM bei der nächsten möglichen Gelegenheit neue IT-Richtlinienregeln hinzugefügt.

Sie können die durchsuchbare und sortierbare Tabelle der IT-Richtlinienregeln herunterladen. In der Tabelle werden alle in UEM verfügbaren Regeln sowie die zur Unterstützung der Regel gültigen Mindestanforderungen an das Betriebssystem dokumentiert.

Das Geräteverhalten, das Sie mit einer IT-Richtlinie steuern, umfasst die folgenden Optionen:

- Kennwortanforderungen an das Gerät
- Die Zulässigkeit von Gerätefunktionen wie Kamera, Bluetooth und Touch ID
- Die Zulässigkeit von App Store- und iTunes Store-Käufen und die Einstufung des Inhalts der Käufe als zulässig
- Die Zulässigkeit von System-Apps, z. B. Safari, Siri und FaceTime
- Die Zulässigkeit der Verwendung von iCloud

Weitere Informationen zum Senden von IT-Richtlinien an Geräte finden Sie in der Dokumentation für Administratoren.

Einrichten der iOS Kennwortanforderungen

Sie können wählen, ob Geräte mit iOS und iPadOS ein Kennwort benötigen. Wenn ein Kennwort erforderlich ist, können Sie die Anforderungen für das Kennwort festlegen.

Hinweis: Bei iOS- und iPadOS-Geräten und in einigen Gerätekennwortregeln wird der Begriff „Code“ verwendet. Beide Begriffe „Kennwort“ und „Code“ haben jedoch die gleiche Bedeutung.

Regel	Beschreibung
Kennwort für Gerät erforderlich	Legen Sie fest, ob der Benutzer ein Gerätekennwort einrichten muss.
Einfachen Wert zulassen	Legen Sie fest, ob das Kennwort aufeinanderfolgende und sich wiederholende Zeichen, wie etwa „DEFG“ oder „3333“, enthalten darf.
Alphanumerischer Wert erforderlich	Geben Sie an, ob das Kennwort sowohl Buchstaben als auch Zahlen enthalten muss.
Mindestlänge für Kennwörter	Legen Sie die Mindestlänge des Kennworts fest. Wenn Sie einen Wert eingeben, der kleiner ist als die für das Gerät erforderliche Mindestlänge, wird die Mindestlänge verwendet.
Mindestanzahl an komplexen Zeichen	Legen Sie die Mindestanzahl an nicht alphanumerischen Zeichen fest, die das Gerätekennwort enthalten muss.
Maximales Kennwortalter	Legen Sie fest, wie viele Tage das Kennwort maximal verwendet werden kann.

Regel	Beschreibung
Maximale Zeit für automatische Sperre	Legen Sie den Maximalwert fest, den der Benutzer für die Zeit bis zur automatischen Sperre einstellen kann, also für die Anzahl der Minuten der Benutzerinaktivität, die verstreichen müssen, bevor das Gerät gesperrt wird. Wenn „Keine“ eingestellt ist, sind auf dem Gerät alle unterstützten Werte verfügbar. Wenn der ausgewählte Wert außerhalb des vom Gerät unterstützten Bereichs liegt, nutzt das Gerät den nächsten unterstützten Wert.
Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter das Gerät maximal prüft, um zu verhindern, dass ein Kennwort erneut verwendet wird.
Maximale Übergangsfrist für Gerätesperre	Legen Sie den Maximalwert fest, den der Benutzer für die Übergangsfrist der Gerätesperre einstellen kann, also für die Zeit, die ein Gerät gesperrt sein kann, bevor zum Entsperren ein Kennwort erforderlich ist. Wenn "Keine" eingestellt ist, sind auf dem Gerät alle Werte verfügbar. Wenn „Sofort“ eingestellt ist, ist sofort nach Sperren des Geräts zum Entsperren das Kennwort erforderlich.
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor das Gerät bereinigt wird.
Kennwortänderungen zulassen (nur unter Aufsicht)	Legen Sie fest, ob ein Benutzer das Kennwort hinzufügen, ändern oder entfernen kann.

Weitere Informationen zu den IT-Richtlinien für Kennwortregeln finden Sie in der Richtlinien-Referenztabelle.

Steuerung von Geräten mithilfe von Profilen

BlackBerry UEM enthält mehrere Profile, mit denen Sie verschiedene iOS- und iPadOS-Gerätefunktionen steuern können. Am häufigsten werden die folgenden Profile verwendet:

Profilname	Beschreibung	Konfigurieren
Aktivierung	Gibt die Geräteaktivierungseinstellungen für Benutzer an, z. B. den Aktivierungstyp, die Methode oder die Anzahl und Typen der Geräte, die ein Benutzer aktivieren kann.	Erstellen eines Aktivierungsprofils
Wi-Fi	Gibt die Einstellungen für Geräte an, um eine Verbindung zu Ihrem geschäftlichen Wi-Fi-Netzwerk herzustellen.	Erstellen eines Wi-Fi-Profils
VPN	Gibt die Einstellungen für Geräte an, um eine Verbindung zu einem geschäftlichen VPN herzustellen.	Erstellen eines VPN-Profils
Proxy	Gibt an, wie Geräte einen Proxyserver für den Zugriff auf Webdienste im Internet oder in einem geschäftlichen Netzwerk verwenden.	Erstellen eines Proxy-Profils
E-Mail	Gibt an, wie Geräte eine Verbindung zum geschäftlichen E-Mail-Server herstellen und E-Mail-Nachrichten, Kalendereinträge und Terminplanerdaten synchronisieren. Wenn Sie BlackBerry Work auf Geräten installieren und konfigurieren, müssen Sie kein E-Mail-Profil einrichten.	Erstellen eines E-Mail-Profils
BlackBerry Dynamics	Ermöglicht Geräten den Zugriff auf BlackBerry Dynamics-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect.	Erstellen eines BlackBerry Dynamics-Profils
BlackBerry Dynamics-Verbindungen	Definiert die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.	Erstellen eines BlackBerry Dynamics-Verbindungsprofils
Konformität	Definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind, und legt entsprechende Durchsetzungsaktionen fest.	Erstellen eines Kompatibilitätsprofils
Enterprise-Konnektivität	Gibt an, ob Geräte BlackBerry Secure Connect Plus verwenden können.	BlackBerry Secure Connect Plus aktivieren

Profilname	Beschreibung	Konfigurieren
Zertifizierungsstellenzer	Gibt ein Zertifizierungsstellenzertifikat an, das von Geräten verwendet werden kann, um vertrauenswürdige Verbindungen mit einem geschäftlichen Netzwerk oder einem Server herzustellen.	Erstellen eines Profils mit Zertifizierungsstellenzertifikat
Benutzeranmeldeinformationen	Gibt an, wie Geräte Clientzertifikate für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abrufen.	Erstellen eines Profils mit Benutzeranmeldeinformationen
SCEP	Gibt den SCEP-Server an, den Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	Erstellen eines SCEP-Profils

Weitere Informationen zum Senden von Profilen an Geräte finden Sie in der Dokumentation für Administratoren.

Profilreferenz – iOS-Geräte

In der folgenden Tabelle sind alle BlackBerry UEM-Profile aufgeführt, die auf iOS- und iPadOS-Geräten unterstützt werden:

Profilname	Beschreibung	Konfigurieren
Richtlinie		
Aktivierung	Gibt die Geräteaktivierungseinstellungen für Benutzer wie den Aktivierungstyp sowie die Anzahl und Typen der Geräte an.	Erstellen eines Aktivierungsprofils
BlackBerry Dynamics	Ermöglicht Geräten den Zugriff auf BlackBerry Dynamics-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect.	Erstellen eines BlackBerry Dynamics-Profils
App-Sperrmodus	Geben Sie eine einzelne App an, die auf Geräten ausgeführt werden soll. Nur Geräte unter Aufsicht.	Erstellen eines Profils für den App-Sperrmodus
Enterprise Management Agent	Gibt an, wann Geräte eine Verbindung mit BlackBerry UEM herstellen, um für die App oder Konfiguration Updates zu erhalten, wenn keine Push-Benachrichtigung verfügbar ist.	Erstellen eines Enterprise Management Agent-Profils
Konformität		
Konformität	Definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind, und legt entsprechende Durchsetzungsaktionen fest.	Erstellen eines Kompatibilitätsprofils

Profilname	Beschreibung	Konfigurieren
Konformität (BlackBerry Dynamics)	Dieses schreibgeschützte Profil zeigt die Konformitätseinstellungen an, die aus Good Control in eine lokale BlackBerry UEM-Umgebung importiert wurden.	Verwalten der BlackBerry Dynamics-Kompatibilitätsprofile
E-Mail, Kalender und Kontakte		
E-Mail	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen E-Mail-Server herstellen und E-Mail-Nachrichten, Kalendereinträge und Terminplanerdaten mithilfe von Exchange ActiveSync oder IBM Notes Traveler synchronisieren.	Erstellen eines E-Mail-Profils
IMAP/POP3-E-Mail	Gibt an, wie Geräte eine Verbindung mit einem IMAP- oder POP3-Mailserver herstellen und wie E-Mail-Nachrichten synchronisiert werden.	Erstellen eines IMAP/POP3-E-Mail-Profils
Gatekeeping	Gibt die Microsoft Exchange-Server für das automatische Gatekeeping an.	Erstellen eines Gatekeeping-Profils
CalDAV	Gibt die Servereinstellungen an, die Geräte verwenden können, um die Kalenderdaten zu synchronisieren.	Erstellen eines CalDAV-Profils
CardDAV	Gibt die Servereinstellungen an, die Geräte verwenden können, um die Kontaktdaten zu synchronisieren.	Erstellen eines CardDAV-Profils
Netzwerke und Verbindungen		
Wi-Fi	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen Wi-Fi-Netzwerk herstellen.	Erstellen eines Wi-Fi-Profils
VPN	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen VPN herstellen.	Erstellen eines VPN-Profils
Proxy	Gibt an, wie Geräte einen Proxyserver für den Zugriff auf Webdienste im Internet oder in einem geschäftlichen Netzwerk verwenden.	Erstellen eines Proxy-Profils
Enterprise-Konnektivität	Gibt an, ob Geräte BlackBerry Secure Connect Plus verwenden können.	BlackBerry Secure Connect Plus aktivieren
BlackBerry Dynamics-Verbindungen	Definiert die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.	Erstellen eines BlackBerry Dynamics-Verbindungsprofils

Profilname	Beschreibung	Konfigurieren
BlackBerry 2FA	Ermöglicht den Einsatz der Zwei-Faktor-Authentifizierung für Benutzer und legt die Konfiguration der Funktionen für die Vorauthentifizierung und Wiederherstellung fest.	Erstellen eines BlackBerry 2FA-Profils
Netzwerknutzung	Sie können steuern, ob geschäftliche Apps das Mobilfunknetz oder Datenroaming verwenden dürfen.	Erstellen eines Netzwerknutzungsprofils
Webinhaltsfilter	Begrenzt die Websites, die Benutzer auf Geräten unter Aufsicht anzeigen können. Nur Geräte unter Aufsicht.	Erstellen von Webinhaltsfilter-Profilen
SSO-Erweiterung	Ermöglicht Geräten die Authentifizierung mittels einmaliger Anmeldung.	SSO-Erweiterungsprofil erstellen
Verwaltete Domänen	Konfiguriert Geräte so, dass Benutzer benachrichtigt werden, wenn sie E-Mails außerhalb von vertrauenswürdigen Domänen senden, und schränkt die Apps ein, die aus internen Domänen heruntergeladene Dokumente anzeigen können.	Erstellen eines Profils für verwaltete Domänen
AirPrint	Ermöglicht Ihnen das Hinzuzufügen von Druckern zu AirPlay-Druckerlisten von Benutzern.	Erstellen eines AirPrint-Profils
AirPlay	Ermöglicht Ihnen das Hinzuzufügen von Geräten zu AirPlay-Gerätelisten von Benutzern.	Erstellen eines AirPlay-Profils
Schutz		
Microsoft Intune-App-Schutz	Ermöglicht die Verwaltung von mit Microsoft Intune geschützten Apps.	Erstellen eines Microsoft Intune-App-Schutzprofils
Standortdienst	Ermöglicht Ihnen, den Standort von Geräten anzufordern und die ungefähren Standorte auf einer Karte anzuzeigen.	Erstellen eines Profils für die Standortbestimmung
Nicht stören	Ermöglicht das Blockieren von BlackBerry Work for iOS-Benachrichtigungen außerhalb der Arbeitstage und -stunden, die Sie festlegen.	Erstellen Sie ein Nicht stören-Profil
Benutzerdefiniert		
Gerät	Ermöglicht die Konfiguration der Informationen, die auf Geräten angezeigt werden.	Erstellen eines Geräteprofils

Profilname	Beschreibung	Konfigurieren
Benutzerdefinierte Payload	Gibt benutzerdefinierte Konfigurationsinformationen mithilfe des Payload-Codes für Geräte an.	Benutzerdefiniertes Payload-Profil erstellen
Per-App-Benachrichtigung	Ermöglicht die Konfiguration der Benachrichtigungseinstellungen für System-Apps und mit BlackBerry UEM verwaltete Apps. Nur Geräte unter Aufsicht.	Erstellen eines Per-App-Benachrichtigungsprofils
Zertifikate		
Zertifizierungsstellenzertifikat	Gibt ein Zertifizierungsstellenzertifikat an, das von Geräten verwendet werden kann, um vertrauenswürdige Verbindungen mit einem geschäftlichen Netzwerk oder einem Server herzustellen.	Erstellen eines Profils mit Zertifizierungsstellenzertifikat
Freigegebenes Zertifikat	Gibt ein Clientzertifikat an, das Geräte für die Authentifizierung von Benutzern mit einem geschäftlichen Netzwerk oder Server verwenden können.	Erstellen eines Profils für ein freigegebenes Zertifikat
Benutzeranmeldeinformationen	Gibt die Zertifizierungsstellenverbindung an, die Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	Erstellen eines Profils mit Benutzeranmeldeinformationen
SCEP	Gibt den SCEP-Server an, den Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	Erstellen eines SCEP-Profils

Verwalten von Apps auf Geräten

Sie können eine Bibliothek mit Apps erstellen, die Sie auf Geräten verwalten und überwachen möchten. BlackBerry UEM bietet die folgenden Optionen für die Verwaltung von Apps auf iOS- und iPadOS-Geräten:

- Sie können öffentliche Apps von App Store als optional oder auf Geräten erforderlich zuweisen.
- Sie können benutzerdefinierte Apps auf UEM hochladen und sie als optionale oder erforderliche Apps bereitstellen.
- Konfigurieren Sie App-Einstellungen wie Verbindungseinstellungen vor, wenn dies von der App zugelassen wird.
- Blockieren Sie den Zugriff von Benutzern auf bestimmte Apps, oder konfigurieren Sie eine Liste zulässiger Apps, und blockieren Sie alle anderen Apps.
- Sie können Apple VPP-Konten mit UEM verknüpfen, sodass Sie gekaufte Lizenzen für mit VPP-Konten verknüpfte Apps verteilen können.
- Konfigurieren Sie öffentliche, ISV- und benutzerdefinierte BlackBerry Dynamics-Apps, um Benutzern den Zugriff auf geschäftliche Ressourcen zu ermöglichen.
- Verbinden Sie UEM mit Microsoft Intune, um die Intune-App-Schutzrichtlinien direkt in der UEM-Verwaltungskonsole festzulegen und Office 365-Apps bereitzustellen und zu verwalten.
- Zeigen Sie die Liste der auf den Geräten installierten persönlichen Apps an.
- Lassen Sie zu, dass Benutzer Apps bewerten und überprüfen für andere Benutzer in Ihrer Umgebung.
- Konfigurieren Sie Benachrichtigungseinstellungen für System-Apps und Apps, die Sie mit UEM verwalten.
- Geben Sie das Symbol und die Bezeichnung für das Symbol „ geschäftliche Apps“ auf Geräten an.

App-Verhalten auf iOS-Geräten mit MDM-Steuerelemente-Aktivierungen

Auf Geräten mit BlackBerry Dynamics-Aktivierung wird der Katalog für geschäftliche Apps in BlackBerry Dynamics Launcher angezeigt, wenn Sie dem Benutzer die Berechtigung „Funktion -BlackBerry App Store“ zugewiesen haben. Weitere Informationen finden Sie unter Hinzufügen des Katalogs mit geschäftlichen Apps zu BlackBerry Dynamics Launcher.

Bei iOS- und iPadOS-Geräten, die mit MDM-Steuerelemente aktiviert wurden, tritt folgendes Verhalten auf:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	Auf beaufsichtigten Geräten werden Apps automatisch installiert. Wenn die App bereits installiert ist, wird sie von UEM verwaltet. Auf nicht beaufsichtigten Geräten wird der Benutzer zur Installation der Apps aufgefordert. Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (auch wenn die App nicht installiert ist) oder wenn der Benutzer die App installiert. Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.	iTunes benachrichtigt Benutzer über verfügbare Updates. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert. (Das kann bis zu einer Stunde dauern.) Auf Geräten, die nicht über Zugriff auf iTunes verfügen, erhalten Benutzer keine Benachrichtigung, können das Update aber aus dem App-Katalog herunterladen, wenn dem Gerät eine Apple-VPP-Lizenz zugewiesen ist.	Apps werden automatisch ohne Benachrichtigung entfernt. Apps werden nicht mehr im App-Katalog angezeigt.	Apps werden automatisch entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Öffentliche Apps mit Verfügbarkeitseins „Optional“	Wenn Apps bereits auf überwachten Geräten installiert sind, wird die App von UEM verwaltet. Auf nicht beaufsichtigten Geräten wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen. Benutzer werden über Änderungen am App-Katalog benachrichtigt. Apps werden aus der Liste „Neuigkeiten und Updates“ nur dann entfernt, wenn der Benutzer die Details anzeigt (unabhängig davon, ob die entsprechende App installiert wurde). Benutzer können wählen, ob sie die Apps installieren möchten.	iTunes benachrichtigt Benutzer über verfügbare Updates. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (unabhängig davon, ob die entsprechende App aktualisiert wurde).	Apps werden automatisch ohne Benachrichtigung entfernt. Apps werden nicht mehr im App-Katalog angezeigt.	Apps werden automatisch entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	Auf beaufsichtigten Geräten werden Apps automatisch installiert. Wenn die App bereits installiert ist, wird sie von UEM verwaltet. Auf nicht beaufsichtigten Geräten wird der Benutzer zur Installation der Apps aufgefordert. Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen. Wenn der Benutzer die Installation abbricht, können Apps aus dem App-Katalog installiert werden. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (auch wenn die App nicht installiert ist) oder wenn der Benutzer die App installiert. Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	Apps werden automatisch ohne Benachrichtigung entfernt. Apps werden nicht mehr im App-Katalog angezeigt.	Apps werden automatisch entfernt.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Interne Apps mit Verfügbarkeitseins „Optional“	Wenn Apps bereits auf überwachten Geräten installiert sind, wird die App von UEM verwaltet. Auf nicht beaufsichtigten Geräten wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (auch wenn die App nicht installiert ist) oder wenn der Benutzer die App installiert.	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	Apps werden auf Geräten, die mit MDM-Steuerelemente aktiviert wurden, ohne Benachrichtigung automatisch entfernt. Apps werden nicht von Geräten entfernt, die mit Privatsphäre des Benutzers aktiviert wurden. Apps werden nicht mehr im App-Katalog angezeigt.	Apps werden automatisch entfernt.

Weitere Informationen zum Verhalten der Eingabeaufforderung bei der Installation von Apps finden Sie unter Hinzufügen einer iOS-App zur App-Liste.

App-Verhalten auf iOS-Geräten mit Privatsphäre des Benutzers-Aktivierungen

Auf Geräten mit BlackBerry Dynamics-Aktivierung wird der Katalog für geschäftliche Apps in BlackBerry Dynamics Launcher angezeigt, wenn Sie dem Benutzer die Berechtigung „Funktion -BlackBerry App Store“ zugewiesen haben. Weitere Informationen finden Sie unter Hinzufügen des Katalogs mit geschäftlichen Apps zu BlackBerry Dynamics Launcher.

Wenn Sie iOS- und iPadOS-Geräte mit Privatsphäre des Benutzers aktivieren, können Sie auswählen, ob die App-Verwaltung zugelassen werden soll. Wenn Sie die App-Verwaltung zulassen, ist das App-Verhalten für Privatsphäre des Benutzers-Aktivierungen dasselbe wie für die Aktivierungsart MDM-Steuerelemente. Wenn Sie die App-Verwaltung für Geräte, die mit Privatsphäre des Benutzers aktiviert wurden, nicht zulassen, tritt das folgende Verhalten auf:

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Öffentliche Apps mit Verfügbarkeitseinstellung „Erforderlich“	Der Benutzer wird nicht aufgefordert, Apps zu installieren. Benutzer müssen zum App-Katalog navigieren, um die gewünschten Apps zu installieren. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (auch wenn die App nicht installiert ist) oder wenn der Benutzer die App installiert.	iTunes benachrichtigt Benutzer über verfügbare Updates. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert. (Das kann bis zu einer Stunde dauern.) Auf Geräten, die nicht über Zugriff auf iTunes verfügen, erhalten Benutzer keine Benachrichtigung, können das Update aber aus dem App-Katalog herunterladen.	Apps bleiben auf dem Gerät. Apps werden nicht mehr im App-Katalog angezeigt.	Apps bleiben auf dem Gerät.
Öffentliche Apps mit Verfügbarkeitsein „Optional“	Wenn die App bereits installiert ist, passiert nichts. Benutzer werden über Änderungen am App-Katalog benachrichtigt. Apps werden aus der Liste „Neuigkeiten und Updates“ nur dann entfernt, wenn der Benutzer die Details anzeigt (unabhängig davon, ob die entsprechende App installiert wurde). Benutzer können wählen, ob sie die Apps installieren möchten.	iTunes benachrichtigt Benutzer über verfügbare Updates. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (unabhängig davon, ob die entsprechende App aktualisiert wurde).	Apps bleiben auf dem Gerät. Apps werden nicht mehr im App-Katalog angezeigt.	Apps bleiben auf dem Gerät.

App-Typ	Verhalten bei App-Zuweisung	Verhalten bei App-Aktualisierung	Verhalten bei Aufhebung der App-Zuweisung	Verhalten bei Entfernen des Geräts aus BlackBerry UEM
Interne Apps mit Verfügbarkeitseinstellung „Erforderlich“	Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (auch wenn die App nicht installiert ist) oder wenn der Benutzer die App installiert.	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	Apps bleiben auf dem Gerät. Apps werden nicht mehr im App-Katalog angezeigt.	Apps bleiben auf dem Gerät.
Interne Apps mit Verfügbarkeitsein „Optional“	Wenn die Apps bereits installiert sind, passiert nichts. Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (auch wenn die App nicht installiert ist) oder wenn der Benutzer die App installiert.	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	Apps bleiben auf dem Gerät. Apps werden nicht mehr im App-Katalog angezeigt.	Apps bleiben auf dem Gerät.

Weitere Informationen zum Verhalten der Eingabeaufforderung bei der Installation von Apps auf einem Gerät finden Sie unter Hinzufügen einer iOS-App zur App-Liste.

Aktivieren von iOS-Geräten

Wenn ein Benutzer ein iOS- oder iPadOS-Gerät mit BlackBerry UEM aktiviert, wird das Gerät mit BlackBerry UEM verknüpft, damit Sie Geräte verwalten und Benutzer auf ihren Geräten auf geschäftliche Daten zugreifen können.

Sie können sich bei der Vorbereitung von Geräten mit BlackBerry UEM aussuchen, ob Sie Apple Configurator 2 verwenden möchten oder nicht. Weitere Informationen zur Verwendung von Apple Configurator 2 finden Sie unter Aktivieren von iOS-Geräten mit Apple Configurator 2 in der Dokumentation für Administratoren.

Sie können Geräte auch beim Programm zur Geräteregistrierung (DEP, Device Enrollment Program) von Apple registrieren und ihnen mit der BlackBerry UEM-Verwaltungskonsole Registrierungskonfigurationen zuweisen. Registrierungskonfigurationen enthalten zusätzliche Regeln, etwa „Beaufsichtigten Modus aktivieren“, die den Geräten bei der MDM-Registrierung zugewiesen werden. Weitere Informationen finden Sie in der Dokumentation für Administratoren unter Aktivieren von beim DEP registrierten iOS-Geräten.

Wenn Geräte nicht beim DEP registriert sind, können Sie die Aktivierung nicht überwachter Geräte dennoch verhindern, und zwar über die Einstellungen im Aktivierungsprofil.

Aktivierungsarten: iOS-Geräte

Aktivierungsart	Beschreibung
MDM-Steuerelemente	Die Aktivierungsart stellt eine grundlegende Geräteverwaltung mithilfe der durch iOS und iPadOS verfügbaren Gerätesteuerelemente bereit. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten. Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern. Während der Aktivierung müssen Benutzer ein Mobilgeräteverwaltungsprofil auf ihrem Gerät installieren. Um festzulegen, ob BlackBerry UEM die Aktivierung anhand der Geräte-ID einschränken kann, wählen Sie **Nur genehmigte Geräte-IDs zulassen** aus.

Aktivierungsart	Beschreibung
Privatsphäre des Benutzers	Sie können die Privatsphäre des Benutzers-Aktivierungsart verwenden, um die grundlegende Steuerung von Geräten zu ermöglichen, und gleichzeitig sicherstellen, dass die persönlichen Daten des Benutzers privat bleiben. Mit dieser Aktivierungsart wird kein separater Container auf dem Gerät installiert, und es ist keine zusätzliche Sicherheit für geschäftliche Daten vorhanden. Mit Privatsphäre des Benutzers aktivierte Geräte sind auf BlackBerry UEM aktiviert und können Dienste wie Find my Phone und Root Detection nutzen. Administratoren können jedoch keine Geräterichtlinien steuern. **Hinweis:** Um die Lizenzierung auf SIM-Basis zuzulassen, müssen Sie die Option „Zugriff auf SIM-Karten- und Hardwareinformationen zulassen, um die SIM-basierte Lizenzierung zu aktivieren“ im Aktivierungsprofil auswählen. Benutzer müssen ein MDM-Profil installieren, das nur auf die SIM-Karten- und Hardwareinformationen zugreifen kann, die erforderlich sind, um zu prüfen, ob eine entsprechende SIM-Lizenz verfügbar ist (z. B. ICCID und IMEI). Diese Aktivierungsart wird für Apple TV-Geräte nicht unterstützt. Wenn Sie Privatsphäre des Benutzers-Aktivierungen zulassen, wählen Sie die Profile aus, die Sie basierend auf den Anforderungen Ihres Unternehmens auf dem Gerät verwalten möchten. Sie können eine der folgenden Optionen auswählen: • **Zugriff auf SIM-Karten- und Hardwareinformationen zulassen, um die SIM-basierte Lizenzierung zu aktivieren**: Diese Option legt fest, ob BlackBerry UEM auf Informationen zur SIM-Karte und zur Gerätehardware, wie ICCID und IMEI, zugreifen kann, um zu überprüfen, ob eine entsprechende SIM-Lizenz verfügbar ist. • **App-Verwaltung zulassen**: Mit dieser Option wird festgelegt, ob Sie geschäftliche Apps auf dem Gerät installieren oder entfernen und eine Liste der installierten geschäftlichen Apps auf dem Bildschirm mit den Benutzerdetails anzeigen möchten. Sie können auch angeben, ob App-Verknüpfungen zugelassen werden sollen. • **IT-Richtlinienverwaltung zulassen**: Mit dieser Option wird festgelegt, ob Sie einen begrenzten Satz von IT-Richtlinienregeln auf das Gerät anwenden möchten (Kennwortrichtlinien, Screenshots zulassen, Dokumente aus verwalteten Quellen in nicht verwalteten Zielen zulassen und Dokumente aus nicht verwalteten Quellen in verwalteten Zielen zulassen). • **E-Mail-Profilverwaltung zulassen**: Mit dieser Option wird festgelegt, ob die E-Mail-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen. • **WLAN-Profilverwaltung zulassen**: Mit dieser Option wird festgelegt, ob die Wi-Fi-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen. • **VPN-Profilverwaltung zulassen**: Mit dieser Option wird festgelegt, ob die VPN-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen.

Aktivierungsart	Beschreibung
Benutzerdatenschutz - Benutzerregistrierung	Sie können die Aktivierungsart Benutzerdatenschutz - Benutzerregistrierung für iOS- und iPadOS-Geräte verwenden, um sicherzustellen, dass Benutzerdaten privat und von geschäftlichen Daten getrennt bleiben. Bei dieser Aktivierungsart wird ein separater geschäftlicher Bereich auf dem Gerät für geschäftliche Apps und native Notizen, iCloud Drive, E-Mails (Anhänge und vollständige E-Mail-Texte), Kalender (Anhänge) und iCloud Keychain-Apps installiert. Diese Aktivierungsart ermöglicht die Verwendung von App-Verwaltung, IT-Richtlinienverwaltung, E-Mail-Profilen Wi-Fi-Profilen und „VPN pro App“. Administratoren können geschäftliche Daten verwalten (z. B. geschäftliche Daten löschen), ohne dass Auswirkungen auf persönliche Daten erfolgen. Diese Aktivierungsart wird auf nicht überwachten iPhone- und iPad-Geräten unterstützt, auf denen iOS bzw. iPadOS OS 13.1 oder höher ausgeführt wird.
Geräteregistrierung nur für BlackBerry 2FA	Diese Aktivierungsart unterstützt die BlackBerry 2FA-Lösung für Geräte, die nicht von BlackBerry UEM verwaltet werden. Diese Aktivierungsart bietet keine Geräteverwaltung oder Steuerelemente, gestattet Geräten jedoch, die BlackBerry 2FA-Funktion zu verwenden. Um diese Aktivierungsart zu verwenden, müssen Sie Benutzern zudem das BlackBerry 2FA-Profil zuweisen. Wenn ein Gerät aktiviert ist, können Sie begrenzte Geräteinformationen in der Verwaltungskonsole anzeigen. Außerdem können Sie das Gerät über einen Befehl deaktivieren. Diese Aktivierungsart wird nur für Microsoft Active Directory-Benutzer unterstützt. Diese Aktivierungsart wird für Apple TV-Geräte nicht unterstützt. Weitere Informationen finden Sie in der Dokumentation zu BlackBerry 2FA.

Erstellen von Aktivierungsprofilen

Mithilfe von Aktivierungsprofilen können Sie steuern, wie die Geräte aktiviert und verwaltet werden. Ein Aktivierungsprofil gibt an, wie viele Geräte und welche Gerätetypen ein Benutzer aktivieren kann, und welche Aktivierungsart für den jeweiligen Gerätetyp verwendet werden soll.

Sie können Aktivierungsarten verwenden, um zu konfigurieren, wie viel Kontrolle Sie über aktivierte Geräte haben. Vielleicht möchten Sie die vollständige Kontrolle über ein Gerät, das Sie einem Benutzer bereitstellen. Vielleicht möchten Sie sicherstellen, dass sie keine Kontrolle über die persönlichen Daten eines Geräts haben, das einem Benutzer gehört und das er zur Arbeit mitbringt.

Das zugewiesene Aktivierungsprofil gilt nur für Geräte, die der Benutzer aktiviert, nachdem Sie ihm das Profil zugewiesen haben. Geräte, die bereits aktiviert sind, werden nicht automatisch aktualisiert, um dem neuen oder aktualisierten Aktivierungsprofil zu entsprechen.

Wenn Sie in BlackBerry UEM einen Benutzer hinzufügen, wird dem Benutzerkonto das Standard-Aktivierungsprofil zugewiesen. Sie können das Standard-Aktivierungsprofil den Anforderungen entsprechend ändern, oder Sie können ein benutzerdefiniertes Aktivierungsprofil erstellen und dieses Benutzern oder Benutzergruppen zuweisen.

Erstellen eines Aktivierungsprofils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.

2. Klicken Sie auf **Richtlinie > Aktivierung**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie im Feld **Anzahl der Geräte, die ein Benutzer aktivieren kann** die maximale Anzahl von Geräten ein, die der Benutzer aktivieren kann.
6. Wählen Sie in der Dropdown-Liste **Geräteeigentümer** die Standardeinstellung für den Geräteeigentümer aus.
   - Wenn einige Benutzer persönliche Geräte und einige Benutzer geschäftliche Geräte aktivieren, wählen Sie **Nicht angegeben** aus.
   - Wählen Sie **Geschäftlich** aus, wenn die meisten Benutzer geschäftliche Geräte aktivieren.
   - Wählen Sie **Persönlich** aus, wenn die meisten Benutzer ihre persönlichen Geräte aktivieren.
7. Wählen Sie optional einen Organisationshinweis in der Dropdown-Liste **Organisationshinweis zuweisen** aus. Wenn Sie einen Organisationshinweis zuordnen, müssen Benutzer, die iOS-, iPadOS-, macOS oder Windows 10-Geräte aktivieren möchten, die Mitteilung akzeptieren, um den Aktivierungsvorgang abzuschließen.
8. Wählen Sie im Abschnitt **Gerätetypen, die Benutzer aktivieren können** die entsprechenden Geräte-OS-Typen aus. Gerätetypen, die Sie nicht auswählen, werden im Aktivierungsprofil nicht berücksichtigt, und Benutzer können diese Geräte nicht aktivieren.
9. Führen Sie die folgenden Aktionen für jeden Gerätetyp durch, der im Aktivierungsprofil enthalten ist:
   a) Klicken Sie auf die Registerkarte für den Gerätetyp.
   b) Wählen Sie in der Dropdown-Liste **Gerätemodell-Einschränkungen** eine der folgenden Optionen aus:
      - **Keine Einschränkungen**: Benutzer können jedes Gerätemodell aktivieren.
      - **Ausgewählte Gerätemodelle zulassen**: Benutzer können nur die von Ihnen angegebenen Gerätemodelle aktivieren. Verwenden Sie diese Option, um die zulässigen Geräte nur auf einige Modelle zu beschränken.
      - **Ausgewählte Gerätemodelle nicht zulassen**: Benutzer können die von Ihnen angegebenen Gerätemodelle nicht aktivieren. Verwenden Sie diese Option, um die Aktivierung einiger Gerätemodelle oder Geräte bestimmter Hersteller zu blockieren.

      Wenn Sie die Gerätemodelle einschränken, die Benutzer aktivieren können, klicken Sie auf **Bearbeiten**, um die Geräte auszuwählen, die Sie zulassen oder einschränken möchten, und klicken Sie dann auf **Speichern**.
   c) Wählen Sie in der Dropdown-Liste **Zugelassene Mindestversion** die OS-Version aus, die als Mindestanforderung zugelassen ist.

      Viele ältere OS-Versionen werden von BlackBerry UEM nicht mehr unterstützt. Sie müssen nur dann eine mindestens erforderliche Version auswählen, wenn Sie die früheste Version, die derzeit von BlackBerry UEM unterstützt wird, nicht zulassen möchten. Weitere Informationen zu den unterstützten Versionen finden Sie in der Kompatibilitätsmatrix.
   d) Wählen Sie die unterstützten Aktivierungstypen aus.
10. Führen Sie für iOS- und iPadOS-Geräte die folgenden Aktionen durch:
   a) Wenn Sie die Aktivierungsart „Privatsphäre des Benutzers“ auswählen und Sie die SIM-basierte Lizenzierung aktivieren möchten, müssen Sie das Kontrollkästchen **Zugriff auf SIM-Karten- und Hardwareinformationen zulassen, um die SIM-basierte Lizenzierung zu aktivieren** auswählen.
   b) Wenn Sie die Aktivierungsart „Privatsphäre des Benutzers“ ausgewählt haben und bestimmte Funktionen verwalten möchten, aktivieren Sie die entsprechenden Kontrollkästchen. Weitere Informationen zu jeder Option finden Sie unter Aktivierungsarten: iOS-Geräte.
   c) Wenn Sie die Aktivierungstypen „MDM-Steuerelemente“ oder „Privatsphäre des Benutzers“ (mit SIM-basierter Lizenzierung) ausgewählt haben und Sie nur beaufsichtigte Geräte aktivieren möchten, wählen Sie **Aktivierung von Geräten ohne Aufsicht nicht zulassen** aus.
   d) Wählen Sie im Abschnitt **Integritätsprüfung der iOS-App** optional eine der folgenden Nachweismethoden aus:

- **App-Integritätsprüfung bei der Aktivierung der BlackBerry Dynamics-App durchführen**: Verwenden Sie diese Methode, um Prüffragen an Geräte zu senden, wenn sie aktiviert werden, und so die Integrität der geschäftlichen iOS-Apps zu überprüfen.
- **App-Integritätsprüfung regelmäßig durchführen**: Verwenden Sie diese Methode, um Prüffragen an Geräte zu senden und so die Integrität von geschäftlichen iOS-Apps zu überprüfen.

Um eine iOS-App-Integritätsprüfung durchzuführen, müssen Sie CylancePROTECT in Ihrer BlackBerry UEM-Domäne aktivieren. Weitere Informationen finden Sie in der Dokumentation zu CylancePROTECT Mobile.

11. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Legen Sie ggf. eine Rangfolge für die Profile fest.

Aktivierung eines iOS- oder iPadOS-Geräts mit der Aktivierungsart MDM-Steuerelemente

Diese Schritte gelten für iOS- und iPadOS-Geräte, die mit MDM-Steuerelemente oder Privatsphäre des Benutzers mit aktivierten MDM-Optionen aktiviert werden.

Während der Aktivierung müssen Benutzer die BlackBerry UEM Client-App verlassen, um das MDM-Profil manuell zu installieren. Der Sperrmodus muss auf dem Gerät deaktiviert sein (iOS und iPadOS 16 oder höher). Der Sperrmodus verhindert die Installation von Konfigurationsprofilen, die für die Aktivierung erforderlich sind.

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer, oder senden Sie ihm einen Link zum folgenden Workflow: Aktivierung Ihres iOS-Geräts.

Bevor Sie beginnen:

- Wenn der Sperrmodus auf Ihrem Gerät aktiviert ist (iOS und iPadOS 16 oder höher), müssen Sie ihn für die Aktivierung des Geräts deaktivieren. Der Sperrmodus verhindert die Installation von Konfigurationsprofilen, die für die Aktivierung erforderlich sind. Bei Bedarf können Sie den Sperrmodus nach der Aktivierung wieder aktivieren.

1. Installieren Sie den BlackBerry UEM Client auf dem Gerät. Sie können den BlackBerry UEM Client aus dem App Store herunterladen.
2. Tippen Sie auf dem Gerät auf **UEM Client**, und akzeptieren Sie die Lizenzvereinbarung.
3. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Aktivieren Sie das Gerät mit einem QR Code.	**a.** Tippen Sie auf . **b.** Tippen Sie auf **Zulassen**, damit der BlackBerry UEM Client Fotos und Videos aufnehmen kann. **c.** Scannen Sie den QR Code in der Aktivierungs-E-Mail, die Sie erhalten haben.
Manuelles Aktivieren des Geräts	**a.** Geben Sie Ihre geschäftliche E-Mail-Adresse und Ihr Aktivierungskennwort ein. **b.** Geben Sie ggf. die Serveradresse ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service. **c.** Tippen Sie auf **Weiter**.

4. Tippen Sie auf **Zulassen**, um Benachrichtigungen von UEM Client erhalten zu können. Wenn Sie **Nicht zulassen** wählen, wird die vollständige Aktivierung des Geräts verhindert.
5. Wenn Sie aufgefordert werden, ein Konfigurationsprofil zu installieren, tippen Sie auf **OK**.
6. Wenn Sie zum Herunterladen des Konfigurationsprofils aufgefordert werden, tippen Sie auf **Zulassen**.
7. Nachdem der Download abgeschlossen ist, öffnen Sie **Einstellungen**.
8. Tippen Sie auf **Allgemein**, und navigieren Sie zu **Profil- und Geräteverwaltung**.
9. Tippen Sie zum Installieren des Profils auf **BlackBerry UEM-Profil**, und befolgen Sie die Anweisungen auf dem Bildschirm.
10. Kehren Sie nach Abschluss der Installation zur BlackBerry UEM Client-App zurück, um die Aktivierung abzuschließen.
11. Wenn Sie dazu aufgefordert werden, folgen Sie den Anweisungen auf dem Bildschirm, um geschäftliche Apps auf Ihrem Gerät zu installieren.

Wenn Sie fertig sind: Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie die BlackBerry UEM Client-App auf dem Gerät, und tippen Sie auf **Info**. Überprüfen Sie im Abschnitt Aktiviertes Gerät und Kompatibilitätsstatus, ob die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivieren eines iOS- oder iPadOS-Geräts mit Apple-Benutzerregistrierung

Die Apple-Benutzerregistrierung wird nur auf Geräten mit iPad und iPadOS 13.1 oder höher unterstützt.

Um mit der Registrierung zu beginnen, verwenden Benutzer die Kamera-App auf dem Gerät, um einen in der Aktivierungs-E-Mail für die Apple-Benutzerregistrierung bereitgestellten QR Code zu scannen, und das MDM-Profil manuell auf das Gerät herunterzuladen und zu installieren. Zum Aktivieren ihres Geräts melden sich Benutzer bei ihrem verwalteten Apple-ID-Konto an, das mit der E-Mail-Adresse des BlackBerry UEM-Benutzerkontos übereinstimmt. Weisen Sie Benutzern den UEM Client mithilfe einer VPP-Lizenz zu, wenn Sie zulassen möchten, dass Benutzer andere BlackBerry Dynamics-Apps aktivieren, Zertifikate importieren, BlackBerry 2FA-Funktionen und CylancePROTECT verwenden sowie ihren Konformitätsstatus überprüfen können. Die UEM Client-Einrichtung wird gestartet, wenn der Benutzer die Lizenzvereinbarung akzeptiert hat.

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

Bevor Sie beginnen:

- Stellen Sie sicher, dass Sie eine Aktivierungs-E-Mail mit dem QR Code für die Apple-Benutzerregistrierung erhalten haben. Wenn Sie die E-Mail nicht erhalten haben, wenden Sie sich an einen Administrator.
- Wenn das Gerät bereits mit BlackBerry UEM aktiviert ist, müssen Sie das Gerät deaktivieren.
- Deinstallieren Sie den BlackBerry UEM Client.
- Sie müssen über ein verwaltetes Apple ID-Konto verfügen, das über Ihr Unternehmen verwaltet wird.
- Das Gerät darf kein überwachtes Gerät sein. Wenn Ihr Gerät überwacht wird, wird dies in den App-Einstellungen in der Nähe Ihrer Apple ID angezeigt.
- Wenn der Sperrmodus auf Ihrem Gerät aktiviert ist (iOS und iPadOS 16 oder höher), müssen Sie ihn deaktivieren, um das Gerät zu aktivieren. Der Sperrmodus verhindert die Installation von Konfigurationsprofilen, die für die Aktivierung erforderlich sind. Bei Bedarf können Sie den Sperrmodus nach der Aktivierung wieder aktivieren.

1. Öffnen Sie die Aktivierungs-E-Mail mit dem QR Code für die Apple-Benutzerregistrierung. Wenn der QR Code bereits abgelaufen ist, fordern Sie einen neuen Aktivierungscode von BlackBerry UEM Self-Service an, oder wenden Sie sich an Ihren Administrator.
2. Öffnen Sie die Kamera-App auf Ihrem Gerät, und scannen Sie den QR-Code in der Aktivierungs-E-Mail. Wenn Sie dazu aufgefordert werden, tippen Sie auf die Benachrichtigung, um die URL in Safari zu öffnen.
3. Wenn Sie zum Herunterladen des UEM-Konfigurationsprofils aufgefordert werden, tippen Sie auf **Zulassen**.
4. Nachdem der Download abgeschlossen ist, tippen Sie auf **Schließen**.
5. Gehen Sie zu **Einstellungen** > **Allgemein** > **Profil**.
6. Tippen Sie auf **UEM-Profil**.
7. Tippen Sie auf dem Benutzerregistrierungsbildschirm auf **Mein iPhone registrieren** oder **Mein iPad registrieren**.
8. Geben Sie Ihre Kennung ein.
9. Melden Sie sich mit Ihren verwalteten Apple ID-Anmeldeinformationen bei der Apple ID an.
10. Wenn Ihr Administrator Ihnen die BlackBerry UEM Client-App zugewiesen hat, tippen Sie bei Aufforderung auf **Installieren**, oder öffnen Sie „Geschäftliche Apps“.
11. Um die BlackBerry UEM Client-App einzurichten, öffnen Sie sie und akzeptieren Sie die Lizenzvereinbarung. Folgen Sie den Anweisungen auf dem Bildschirm, um den Aktivierungsprozess abzuschließen.

Wenn Sie fertig sind: Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie die BlackBerry UEM Client-App auf dem Gerät, und tippen Sie auf **Info**. Überprüfen Sie im Abschnitt Aktiviertes Gerät und Kompatibilitätsstatus, ob die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

Aktivierte Geräte verwalten und überwachen

Wenn iOS- und iPadOS-Geräte durch eine IT-Richtlinie und Profile aktiviert und verwaltet wurden, stehen Ihnen mehrere Funktionen zur Steuerung der Geräte der Benutzer zur Verfügung.

Sie haben folgende Wahlmöglichkeiten:

Option	Beschreibung
Nach verfügbaren Software-Updates suchen und das Gerät aktualisieren	Sie können für alle verwalteten Geräte die verfügbaren Betriebssystemaktualisierungen anzeigen. Sie können die Installation verfügbarer Updates auf beaufsichtigten Geräten erzwingen. Weitere Informationen finden Sie in der Dokumentation für Administratoren.
Standorteinstellungen und Verloren-Modus aktivieren	Sie können Standorteinstellungen aktivieren, um Geräte zu orten. Sie können auch den Verloren-Modus aktivieren, um nach einem verlorenen Gerät zu suchen. Weitere Informationen finden Sie in der Dokumentation für Administratoren.
Aktivierungssperre aktivieren	Wenn die Aktivierungssperre auf Geräten eingeschaltet ist, müssen Benutzer die Apple-ID und das Kennwort bestätigen, wenn sie die Funktion „Mein iPhone suchen“ deaktivieren, Daten vom Gerät löschen oder das Gerät reaktivieren und verwenden möchten. So verwalten Sie die Aktivierungssperre in BlackBerry UEM: • Das Gerät muss überwacht werden. • Das Gerät muss ein konfiguriertes iCloud-Konto besitzen. • Auf dem Gerät muss „Mein iPhone suchen“ oder „Mein iPad suchen“ aktiviert sein. BlackBerry UEM speichert einen Umgehungscode zum Löschen der Sperre, mit dem sich ohne Eingabe von Apple-ID und Kennwort des Benutzers Daten auf dem Gerät löschen lassen und das Gerät erneut aktiviert werden kann. Weitere Informationen finden Sie in der Dokumentation für Administratoren.
Geräteprotokolle auslesen	Sie können zu Überwachungs- und Fehlerbehebungszwecken Protokolle von Geräten abrufen. Weitere Informationen finden Sie in der Dokumentation für Administratoren.
Gerät deaktivieren	Wenn Sie oder ein Benutzer ein Gerät deaktiviert, wird die Verbindung zwischen dem Gerät und dem Benutzerkonto in BlackBerry UEM entfernt. Sie können das Gerät nicht verwalten, und das Gerät wird nicht mehr in der Verwaltungskonsole angezeigt. Der Benutzer kann nicht auf die geschäftlichen Daten auf dem Gerät zugreifen. Sie können ein Gerät mit dem Befehl „Alle Gerätedaten löschen“ oder „Nur geschäftliche Daten löschen“ deaktivieren. Benutzer können ein Gerät deaktivieren, indem sie auf dem Bildschirm „Info“ in der BlackBerry UEM Client-App „Mein Gerät deaktivieren“ auswählen.

Senden von Befehlen an Geräte

Bevor Sie beginnen:

Wenn Sie ein Ablaufdatum für Befehle einrichten möchten, mit denen Daten aus Geräten in BlackBerry UEM gelöscht werden, lesen Sie den Abschnitt Einrichten eines Ablaufdatums für Befehle.

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzerkontos.
4. Klicken Sie auf die Registerkarte „Gerät“.
5. Wählen Sie im Fenster **Gerät verwalten** den Befehl aus, den Sie an das Gerät senden möchten.

Befehle für iOS-Geräte

Diese Befehle gelten auch für iPadOS-Geräte.

Befehl	Beschreibung	Aktivierungsarten
Anzeigen des Geräteberichts	Durch diesen Befehl werden Detailinformationen zu einem Gerät angezeigt. Sie können den Gerätebericht exportieren und auf Ihrem Computer speichern. Weitere Informationen finden Sie unter Anzeigen und Speichern eines Geräteberichts.	MDM-Steuerelemente Privatsphäre des Benutzers
Anzeigen der Geräteaktionen	Mit diesem Befehl werden alle Aktionen angezeigt, die gerade auf einem Gerät durchgeführt werden. Weitere Informationen finden Sie unter Anzeigen der Geräteaktionen.	MDM-Steuerelemente Privatsphäre des Benutzers
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind. Außerdem wird das Gerät auf die werkseitigen Standardeinstellungen zurückgesetzt. Wenn das Gerät keine Verbindung zu BlackBerry UEM herstellen kann, wenn Sie diesen Befehl senden, können Sie den Befehl entweder abbrechen oder das Gerät aus der Konsole entfernen. Wenn das Gerät eine Verbindung zu BlackBerry UEM herstellt, nachdem Sie es entfernt haben, werden nur die Geschäftsdaten vom Gerät entfernt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente

Befehl	Beschreibung	Aktivierungsarten
Nur geschäftliche Daten löschen	Mit diesem Befehl werden Geschäftsdaten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, vom Gerät gelöscht. Wenn das Gerät keine Verbindung zu BlackBerry UEM herstellen kann, wenn Sie diesen Befehl senden, können Sie den Befehl entweder abbrechen oder das Gerät aus der Konsole entfernen. Wenn das Gerät eine Verbindung zu BlackBerry UEM herstellt, nachdem Sie es entfernt haben, werden die geschäftlichen Daten vom Gerät entfernt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente Privatsphäre des Benutzers
Gerät sperren	Mit diesem Befehl sperren Sie ein Gerät. Der Benutzer muss das bestehende Gerätekennwort eingeben, um das Gerät zu entsperren. Wenn ein Gerät vorübergehend verlegt wurde, können Sie diesen Befehl verwenden. Wenn Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Kennwort entsperren und löschen	Dieser Befehl entsperrt ein Gerät und löscht das bestehende Kennwort. Der Benutzer wird zur Eingabe eines Gerätekennworts aufgefordert. Sie können diesen Befehl verwenden, wenn der Benutzer das Gerätekennwort vergessen hat. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Verloren-Modus aktivieren	Durch diesen Befehl wird das Gerät gesperrt, und Sie können eine Telefonnummer und eine Nachricht festlegen, die auf dem Gerät angezeigt werden sollen. Sie können z. B. Kontaktinformationen anzeigen lassen, für den Fall, dass das Gerät gefunden wird. Nachdem Sie diesen Befehl gesendet haben, können Sie den Standort des Geräts in BlackBerry UEM anzeigen. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
BlackBerry 2FA deaktivieren	Mit diesem Befehl werden Geräte deaktiviert, die mit der Aktivierungsart „BlackBerry 2FA“ aktiviert wurden. Das Gerät wird von BlackBerry UEM entfernt, und der Benutzer kann die Funktion BlackBerry 2FA nicht mehr verwenden. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente

Befehl	Beschreibung	Aktivierungsarten
Betriebssystem aktualisieren	Dieser Befehl erzwingt die Installation eines verfügbaren Betriebssystem-Updates. Weitere Informationen finden Sie unter Aktualisieren des Betriebssystems auf beaufsichtigten iOS-Geräten. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Gerät neu starten	Dieser Befehl erzwingt den Neustart von Geräten. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Gerät abschalten	Dieser Befehl erzwingt das Ausschalten von Geräten. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Apps bereinigen	Mit diesem Befehl werden die Daten von allen mit Microsoft Intune verwalteten Apps auf dem Gerät bereinigt. Die Apps werden nicht vom Gerät entfernt. Weitere Informationen finden Sie unter Von Microsoft Intune verwaltete Apps löschen.	MDM-Steuerelemente
Gerätedaten aktualisieren	Dieser Befehl sendet und empfängt aktualisierte Gerätedaten. Beispielsweise können Sie kürzlich aktualisierte IT-Richtlinienregeln oder Profile an ein Gerät senden und aktualisierte Informationen zu einem Gerät, wie Betriebssystemversion oder Akkuladezustand, empfangen. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente Privatsphäre des Benutzers
Zeitzone aktualisieren	Mit diesem Befehl wird die Zeitzone des Geräts entsprechend der ausgewählten Region festgelegt.	MDM-Steuerelemente

Befehl	Beschreibung	Aktivierungsarten
Gerät entfernen	Dieser Befehl entfernt das Gerät aus BlackBerry UEM, entfernt aber keine Daten vom Gerät. Das Gerät empfängt ggf. weiterhin E-Mails und andere geschäftliche Daten. Dieser Befehl ist für Geräte vorgesehen, die unwiederbringlich verloren gegangen sind oder beschädigt wurden und erwartungsgemäß keine erneute Verbindung zum Server herstellen werden. Wenn ein Gerät, das entfernt wurde, BlackBerry UEM zu kontaktieren versucht, erhält der Benutzer eine Benachrichtigung. Das Gerät kann erst dann wieder mit BlackBerry UEM kommunizieren, wenn es erneut aktiviert wurde. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente Privatsphäre des Benutzers
Aktualisieren von eSIM-Mobilfunkverträgen	Bei Geräten mit einem eSIM-basierten Mobilfunkvertrag fragt dieser Befehl aktualisierte Vertragsdetails für das Gerät über die Betreiber-URL des Geräts ab.	MDM-Steuerelemente

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada