



# **BlackBerry UEM**

## **Verwalten von iOS-Geräten**

Verwalten

12.12



# Contents

<b>Verwalten von iOS-Geräten.....</b>	<b>4</b>
Verwalten anderer Apple-Geräte.....	4
<b>Was Sie auf iOS-Geräten steuern können.....</b>	<b>5</b>
<b>Lizenzen, die von iOS-Geräten verwendet werden.....</b>	<b>7</b>
<b>Schritte zum Verwalten von iOS-Geräten.....</b>	<b>8</b>
<b>Steuerung von iOS-Geräten mit einer IT-Richtlinie.....</b>	<b>9</b>
Einrichten der iOS-Kennwortanforderungen.....	9
<b>Steuern von iOS-Geräten mithilfe von Profilen.....</b>	<b>11</b>
Profilreferenz – iOS-Geräte.....	12
<b>Verwalten von Apps auf iOS-Geräten.....</b>	<b>16</b>
App-Verhalten auf iOS-Geräten mit MDM-Steuerelemente-Aktivierungen.....	16
App-Verhalten auf iOS-Geräten mit Privatsphäre des Benutzers-Aktivierungen.....	20
<b>Aktivieren von iOS-Geräten.....</b>	<b>23</b>
Aktivierungsarten: iOS-Geräte.....	23
Aktivieren eines iOS-Geräts der Version 12.2 oder höher mit dem Aktivierungstyp „MDM-Steuerelemente“.....	25
Aktivieren eines iOS-Geräts vor Version 12.2 mit dem Aktivierungstyp „MDM-Steuerelemente“.....	26
Aktivieren eines iOS- oder iPad OS-Gerät mit Apple-Benutzerregistrierung.....	27
<b>Aktivierte iOS-Geräte verwalten und überwachen.....</b>	<b>29</b>
Befehle für iOS-Geräte.....	30
<b>Rechtliche Hinweise.....</b>	<b>34</b>

# Verwalten von iOS-Geräten

BlackBerry UEM ermöglichen eine präzise Verwaltung der Verbindung von iOS-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.

In diesem Handbuch wird erläutert, welche Optionen Sie zur Verwaltung von iOS-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 unterstützten macOS-Versionen [finden Sie in den Kompatibilitätsmatrizen](#). Um Apple TV-Geräte zu verwalten, befolgen Sie einfach die Anleitung 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-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)	<p>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.</p> <p>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.</p>
Teilweise verwaltete Geräte mit einem geschäftlichen Profil	<p>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.</p> <p>Bei dieser Aktivierungsart wird ein separater geschäftlicher Bereich auf dem Gerät für geschäftliche Apps und native Notizen, iCloud-Laufwerk, E-Mails (Anhänge und vollständige E-Mail-Texte), Kalender (Anhänge) und iCloud Keychain-Apps installiert.</p>
Verwaltete Geräte (Geräte, die von BlackBerry UEM verwaltet werden)	<p>Sie können ein Gerät aktivieren, um es vollständig von BlackBerry UEM zu verwalten. Diese Option wird häufig für unternehmenseigene Geräte verwendet.</p> <p>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.</p> <p>BlackBerry UEM unterstützt die Verwaltung von iOS-Geräten unter Aufsicht. Einige IT-Richtlinienregeln werden nur auf Geräten unter Aufsicht unterstützt.</p>

Privatsphäre des Benutzers-Aktivierungen 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 SIM-Karten- und Hardwareinformationen: BlackBerry UEM-Zugriff auf SIM-Karten- und Hardwareinformationen 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.

Sie können die Aktivierungsart Benutzerdatenschutz - Benutzerregistrierung für iOS- und iPad OS-Geräte verwenden, um sicherzustellen, dass Benutzerdaten privat und von geschäftlichen Daten getrennt bleiben. 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 „Per App VPN“. 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 iPad OS 13.1 oder 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

# Lizenzen, die von iOS-Geräten verwendet werden

Wenn Sie oder Benutzer ein iOS-Gerät mit BlackBerry UEM aktivieren, verknüpfen Sie das Gerät mit BlackBerry UEM, damit Sie die Geräte verwalten und Benutzer auf ihren Geräten auf geschäftliche Daten zugreifen können. Für die meisten iOS-Aktivierungstypen ist mindestens eine Silver BlackBerry UEM-Lizenz oder eine BlackBerry Secure UEM & Productivity Suites – Choice-Lizenz erforderlich. Je nachdem, welche Funktionen Sie für Benutzer aktivieren möchten, sind jedoch möglicherweise weitere Lizenzen erforderlich.

Funktion	Mindestens erforderliche Lizenz
MDM-Steuerelemente- oder Privatsphäre des Benutzers-Aktivierung	Eine der folgenden Bedingungen muss erfüllt sein: <ul style="list-style-type: none"><li>• Silver</li><li>• BlackBerry Secure UEM &amp; Productivity Suites – Choice</li></ul>
BlackBerry Secure Gateway	Eine der folgenden Bedingungen muss erfüllt sein: <ul style="list-style-type: none"><li>• Gold</li><li>• BlackBerry Secure UEM &amp; Productivity Suites – Choice</li></ul> Weitere Informationen zum BlackBerry Secure Gateway finden Sie in der <a href="#">BlackBerry UEM Dokumentation für Administratoren</a> .
BlackBerry Secure Connect Plus	Eine der folgenden Bedingungen muss erfüllt sein: <ul style="list-style-type: none"><li>• Gold</li><li>• BlackBerry Secure UEM &amp; Productivity Suites – Freedom</li></ul> Weitere Informationen zu BlackBerry Secure Connect Plus finden Sie in der <a href="#">BlackBerry UEM Dokumentation für Administratoren</a> .
BlackBerry Access-App	BlackBerry Secure UEM & Productivity Suites – Choice
BlackBerry Work- und BlackBerry Tasks-Apps	BlackBerry Secure UEM & Productivity Suites – Choice
Alle anderen BlackBerry- und ISV BlackBerry Dynamics-Apps	BlackBerry Secure UEM & Productivity Suites – Freedom
Geräteregistrierung nur für BlackBerry 2FA	Eine der folgenden Bedingungen muss erfüllt sein: <ul style="list-style-type: none"><li>• BlackBerry 2FA</li><li>• BlackBerry Secure UEM &amp; Productivity Suites – Freedom</li></ul>

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 <a href="#">Installationsanweisungen</a> . Um iOS-Geräte verwalten zu können, müssen Sie <a href="#">ein APNs-Zertifikat von Apple abrufen</a> .
2	Wenn Ihr Unternehmen das Apple-Programm zur Geräteregistrierung verwendet, <a href="#">konfigurieren Sie BlackBerry UEM für die Verwendung von DEP</a> .
3	Stellen Sie sicher, dass Sie über die <a href="#">entsprechenden Lizenzen zur Aktivierung von iOS-Geräten</a> mit den entsprechenden Funktionen verfügen.
4	Konfigurieren Sie <a href="#">IT-Richtlinien</a> für Geräte. Weisen Sie Benutzergruppen oder einzelnen Benutzern IT-Richtlinien zu.
5	Konfigurieren Sie <a href="#">Profile</a> für Geräte. Weisen Sie Benutzergruppen oder einzelnen Benutzern Profile zu.
6	Wenn Ihr Unternehmen über ein Apple VPP-Konto verfügt, <a href="#">fügen Sie es zu BlackBerry UEM hinzu</a> .
7	Geben Sie die <a href="#">Apps an, die Geräte installieren können oder müssen</a> .
8	<a href="#">Aktivieren Sie Geräte</a> .
9	<a href="#">Verwalten und überwachen Sie Geräte</a> .



# Steuerung von iOS-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 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 durchsuch- 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:

- Die [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 iOS-Geräte ein Kennwort benötigen. Wenn ein Kennwort erforderlich ist, können Sie die Anforderungen für das Kennwort festlegen.

**Hinweis:** Bei iOS-Geräten und in einigen Gerätekenntwortregeln 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 Gerätekenntwort 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 iOS-Gerät erforderliche Mindestlänge, wird die Mindestlänge verwendet.
Mindestanzahl an komplexen Zeichen	Legen Sie die Mindestanzahl an nicht alphanumerischen Zeichen fest, die das Gerätekenntwort 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-Referenztafel](#).

# Steuern von iOS-Geräten mithilfe von Profilen

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

Profilname	Beschreibung	Konfigurieren von
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.	<a href="#">Erstellen eines Aktivierungsprofils</a>
Wi-Fi	Gibt die Einstellungen für Geräte an, um eine Verbindung zu Ihrem geschäftlichen Wi-Fi-Netzwerk herzustellen.	<a href="#">Erstellen eines Wi-Fi-Profiles</a>
VPN	Gibt die Einstellungen für Geräte an, um eine Verbindung zu einem geschäftlichen VPN herzustellen.	<a href="#">Erstellen eines VPN-Profiles</a>
Proxy	Gibt an, wie Geräte einen Proxyserver für den Zugriff auf Webdienste im Internet oder in einem geschäftlichen Netzwerk verwenden.	<a href="#">Erstellen eines Proxy-Profiles</a>
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.	<a href="#">Erstellen eines E-Mail-Profiles</a>
BlackBerry Dynamics	Ermöglicht Geräten den Zugriff auf BlackBerry Dynamics-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect.	<a href="#">Erstellen eines BlackBerry Dynamics-Profiles</a>
BlackBerry Dynamics-Verbindungen	Definiert die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.	<a href="#">Erstellen eines BlackBerry Dynamics-Verbindungsprofils</a>
Konformität	Definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind, und legt entsprechende Durchsetzungsaktionen fest.	<a href="#">Erstellen eines Kompatibilitätsprofils</a>

Profilname	Beschreibung	Konfigurieren von
Enterprise-Konnektivität	Gibt an, ob Geräte BlackBerry Secure Connect Plus verwenden können.	<a href="#">BlackBerry Secure Connect Plus aktivieren</a>
Zertifizierungsstellenzertifikat	Gibt ein Zertifizierungsstellenzertifikat an, das von Geräten verwendet werden kann, um vertrauenswürdige Verbindungen mit einem geschäftlichen Netzwerk oder einem Server herzustellen.	<a href="#">Erstellen eines Profils mit Zertifizierungsstellenzertifikat</a>
Benutzeranmeldeinformationen	Gibt an, wie Geräte Clientzertifikate für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abrufen.	<a href="#">Erstellen eines Profils mit Benutzeranmeldeinformationen</a>
SCEP	Gibt den SCEP-Server an, den Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	<a href="#">Erstellen eines SCEP-Profiles</a>

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-Geräten unterstützt werden:

Profilname	Beschreibung	Konfigurieren von
<b>Richtlinie</b>		
Aktivierung	Gibt die Geräteaktivierungseinstellungen für Benutzer wie den Aktivierungstyp sowie die Anzahl und Typen der Geräte an.	<a href="#">Erstellen eines Aktivierungsprofils</a>
BlackBerry Dynamics	Ermöglicht Geräten den Zugriff auf BlackBerry Dynamics-Apps wie BlackBerry Work, BlackBerry Access und BlackBerry Connect.	<a href="#">Erstellen eines BlackBerry Dynamics-Profiles</a>
App-Sperrmodus	Geben Sie eine einzelne App an, die auf Geräten ausgeführt werden soll. Nur iOS-Geräte unter Aufsicht.	<a href="#">Erstellen eines Profils für den App-Sperrmodus</a>
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.	<a href="#">Erstellen eines Enterprise Management Agent-Profiles</a>

Profilname	Beschreibung	Konfigurieren von
<b>Konformität</b>		
Konformität	Definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind, und legt entsprechende Durchsetzungsaktionen fest.	<a href="#">Erstellen eines Kompatibilitätsprofils</a>
Konformität (BlackBerry Dynamics)	Dieses schreibgeschützte Profil zeigt die Konformitätseinstellungen an, die aus Good Control in eine lokale BlackBerry UEM-Umgebung importiert wurden.	<a href="#">Verwalten der BlackBerry Dynamics-Kompatibilitätsprofile</a>
<b>E-Mail, Kalender und Kontakte</b>		
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.	<a href="#">Erstellen eines E-Mail-Profiles</a>
IMAP/POP3-E-Mail	Gibt an, wie Geräte eine Verbindung mit einem IMAP- oder POP3-Mailserver herstellen und wie E-Mail-Nachrichten synchronisiert werden.	<a href="#">Erstellen eines IMAP/POP3-E-Mail-Profiles</a>
Gatekeeping	Gibt die Microsoft Exchange-Server für das automatische Gatekeeping an.	<a href="#">Erstellen eines Gatekeeping-Profiles</a>
CalDAV	Gibt die Servereinstellungen an, die Geräte verwenden können, um die Kalenderdaten zu synchronisieren.	<a href="#">Erstellen eines CalDAV-Profiles</a>
CardDAV	Gibt die Servereinstellungen an, die Geräte verwenden können, um die Kontaktdaten zu synchronisieren.	<a href="#">Erstellen eines CardDAV-Profiles</a>
<b>Netzwerke und Verbindungen</b>		
Wi-Fi	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen Wi-Fi-Netzwerk herstellen.	<a href="#">Erstellen eines Wi-Fi-Profiles</a>
VPN	Gibt an, wie Geräte eine Verbindung mit einem geschäftlichen VPN herstellen.	<a href="#">Erstellen eines VPN-Profiles</a>
Proxy	Gibt an, wie Geräte einen Proxyserver für den Zugriff auf Webdienste im Internet oder in einem geschäftlichen Netzwerk verwenden.	<a href="#">Erstellen eines Proxy-Profiles</a>

Profilname	Beschreibung	Konfigurieren von
Enterprise-Konnektivität	Gibt an, wie Geräte mithilfe der Enterprise-Konnektivität eine Verbindung mit den Ressourcen Ihres Unternehmens herstellen können. Bei iOS-Geräten gibt das Enterprise-Konnektivitätsprofil an, ob Geräte BlackBerry Secure Connect Plus verwenden können.	<a href="#">BlackBerry Secure Connect Plus aktivieren</a>
BlackBerry Dynamics-Verbindungen	Definiert die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.	<a href="#">Erstellen eines BlackBerry Dynamics-Verbindungsprofils</a>
BlackBerry 2FA	Ermöglicht den Einsatz der Zwei-Faktor-Authentifizierung für Benutzer und legt die Konfiguration der Funktionen für die Vorauthentifizierung und Wiederherstellung fest.	<a href="#">Erstellen eines BlackBerry 2FA-Profiles</a>
Netzwerknutzung	Sie können steuern, ob geschäftliche Apps auf iOS-Geräten das Mobilfunknetz oder Datenroaming verwenden dürfen.	<a href="#">Erstellen eines Netzwerknutzungsprofils</a>
Webinhaltsfilter	Begrenzt die Websites, die ein Benutzer auf überwachten iOS-Geräten anzeigen kann.  Nur iOS-Geräte unter Aufsicht.	<a href="#">Erstellen von Webinhaltsfilter-Profilen</a>
Einmalige Anmeldung	Gibt an, wie Geräte bei sicheren Domänen automatisch eine Authentifizierung durchführen, nachdem die Benutzer zum ersten Mal ihren Benutzernamen und ihr Kennwort eingegeben haben.	<a href="#">Erstellen eines Profils für die einmalige Anmeldung</a>
Verwaltete Domänen	Konfiguriert iOS-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.	<a href="#">Erstellen eines Profils für verwaltete Domänen</a>
AirPrint	Ermöglicht Ihnen das Hinzufügen von Druckern zu AirPlay-Druckerlisten von Benutzern.	<a href="#">Erstellen eines AirPrint-Profiles</a>
AirPlay	Ermöglicht Ihnen das Hinzufügen von Geräten zu AirPlay-Gerätelisten von Benutzern.	<a href="#">Erstellen eines AirPlay-Profiles</a>
SSO-Erweiterung	Ermöglicht die SSO-Authentifizierung von Geräten mit iOS (oder iPadOS) 13 oder höher.	<a href="#">SSO-Erweiterungsprofil erstellen</a>

Profilname	Beschreibung	Konfigurieren von
<b>Schutz</b>		
Microsoft Intune-App-Schutz	Ermöglicht die Verwaltung von mit Microsoft Intune geschützten Apps.	<a href="#">Erstellen eines Microsoft Intune-App-Schutzprofils</a>
Standortdienst	Ermöglicht Ihnen, den Standort von Geräten anzufordern und die ungefähren Standorte auf einer Karte anzuzeigen.	<a href="#">Erstellen eines Profils für die Standortbestimmung</a>
Nicht stören	Ermöglicht das Blockieren von BlackBerry Work for iOS-Benachrichtigungen an Tagen und Uhrzeiten außerhalb der Arbeit, die Sie festlegen.	<a href="#">Erstellen Sie ein Nicht stören-Profil</a>
<b>Benutzerdefiniert</b>		
Gerät	Ermöglicht die Konfiguration der Informationen, die auf Geräten angezeigt werden.	<a href="#">Erstellen eines Geräteprofils</a>
Benutzerdefinierte Payload	Gibt benutzerdefinierte Konfigurationsinformationen mithilfe des Payload-Codes für Geräte an.	<a href="#">Benutzerdefiniertes Payload-Profil erstellen</a>
Per-App-Benachrichtigung	Ermöglicht die Konfiguration der Benachrichtigungseinstellungen für System-Apps und mit BlackBerry UEM verwaltete Apps. Nur iOS-Geräte unter Aufsicht.	<a href="#">Erstellen eines Per-App-Benachrichtigungsprofils</a>
<b>Zertifikate</b>		
Zertifizierungsstellenzer	Gibt ein Zertifizierungsstellenzertifikat an, das von Geräten verwendet werden kann, um vertrauenswürdige Verbindungen mit einem geschäftlichen Netzwerk oder einem Server herzustellen.	<a href="#">Erstellen eines Profils mit Zertifizierungsstellenzertifikat</a>
Freigegebenes Zertifikat	Gibt ein Clientzertifikat an, das Geräte für die Authentifizierung von Benutzern mit einem geschäftlichen Netzwerk oder Server verwenden können.	<a href="#">Erstellen eines Profils für ein freigegebenes Zertifikat</a>
Benutzeranmeldeinform	Gibt die Zertifizierungsstellenverbindung an, die Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	<a href="#">Erstellen eines Profils mit Benutzeranmeldeinformationen</a>
SCEP	Gibt den SCEP-Server an, den Geräte verwenden, um ein Clientzertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	<a href="#">Erstellen eines SCEP-Profiles</a>

# Verwalten von Apps auf iOS-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-Geräten:

- [Weisen Sie öffentliche Apps](#) von App Store als optional oder auf Geräten erforderlich zu.
- [Laden Sie benutzerdefinierte Apps](#) auf UEM hoch, und stellen Sie sie als optionale oder erforderliche Apps bereit.
- [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-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“	<p>Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen.</p> <p>Auf beaufsichtigten Geräten werden Apps automatisch installiert.</p> <p>Auf nicht beaufsichtigten Geräten wird der Benutzer zur Installation der Apps aufgefordert.</p> <p>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.</p> <p>Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.</p>	<p>iTunes benachrichtigt Benutzer über verfügbare Updates.</p> <p>Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert. (Das kann bis zu einer Stunde dauern.)</p> <p>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.</p>	<p>Apps werden automatisch ohne Benachrichtigung entfernt.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	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 Verfügbarkeitseinstellung „Optional“	<p>Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen.</p> <p>Benutzer werden über Änderungen am App-Katalog benachrichtigt.</p> <p>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).</p> <p>Benutzer können wählen, ob sie die Apps installieren möchten.</p>	<p>iTunes benachrichtigt Benutzer über verfügbare Updates.</p> <p>Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (unabhängig davon, ob die entsprechende App aktualisiert wurde).</p>	<p>Apps werden automatisch ohne Benachrichtigung entfernt.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	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“	<p>Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen.</p> <p>Auf beaufsichtigten Geräten werden Apps automatisch installiert.</p> <p>Auf nicht beaufsichtigten Geräten werden Benutzer zur Installation der Apps aufgefordert. Wenn der Benutzer die Installation abbricht, können Apps aus dem App-Katalog installiert werden.</p> <p>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.</p> <p>Sie können mit einem Kompatibilitätsprofil die Aktionen definieren, die eintreten, wenn erforderliche Apps nicht installiert werden.</p>	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	<p>Apps werden automatisch ohne Benachrichtigung entfernt.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	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 „Optional“	<p>Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen.</p> <p>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.</p>	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	<p>Apps werden auf Geräten, die mit MDM-Steuerelemente aktiviert wurden, ohne Benachrichtigung automatisch entfernt.</p> <p>Apps werden nicht von Geräten entfernt, die mit Privatsphäre des Benutzers aktiviert wurden.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	Apps werden automatisch entfernt.

## 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-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 iOS-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“	<p>Der Benutzer wird nicht aufgefordert, Apps zu installieren. Benutzer müssen zum App-Katalog navigieren, um die gewünschten Apps zu installieren.</p> <p>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.</p>	<p>iTunes benachrichtigt Benutzer über verfügbare Updates.</p> <p>Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert. (Das kann bis zu einer Stunde dauern.)</p> <p>Auf Geräten, die nicht über Zugriff auf iTunes verfügen, erhalten Benutzer keine Benachrichtigung, können das Update aber aus dem App-Katalog herunterladen.</p>	<p>Apps bleiben auf dem Gerät.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	Apps bleiben auf dem Gerät.
Öffentliche Apps mit Verfügbarkeitseinstellung „Optional“	<p>Wenn die App bereits installiert ist, passiert nichts.</p> <p>Benutzer werden über Änderungen am App-Katalog benachrichtigt.</p> <p>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).</p> <p>Benutzer können wählen, ob sie die Apps installieren möchten.</p>	<p>iTunes benachrichtigt Benutzer über verfügbare Updates.</p> <p>Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die Details anzeigt (unabhängig davon, ob die entsprechende App aktualisiert wurde).</p>	<p>Apps bleiben auf dem Gerät.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	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“	<p>Wenn die Apps bereits installiert sind, wird der Benutzer aufgefordert, die Verwaltung von Apps über UEM zuzulassen.</p> <p>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.</p>	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	<p>Apps bleiben auf dem Gerät.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	Apps bleiben auf dem Gerät.
Interne Apps mit Verfügbarkeitsein „Optional“	<p>Wenn die Apps bereits installiert sind, passiert nichts.</p> <p>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.</p>	Apps werden aus der Liste „Neuigkeiten und Updates“ entfernt, wenn der Benutzer die App aktualisiert.	<p>Apps bleiben auf dem Gerät.</p> <p>Apps werden nicht mehr im App-Katalog angezeigt.</p>	Apps bleiben auf dem Gerät.

# Aktivieren von iOS-Geräten

Wenn Sie oder Benutzer ein iOS-Gerät mit BlackBerry UEM aktivieren, verknüpfen Sie das Gerät mit BlackBerry UEM, damit Sie die 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 iOS-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	<p>Diese Aktivierungsart stellt eine grundlegende Geräteverwaltung über die von iOS zur Verfügung gestellten Gerätesteuerelemente bereit. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten.</p> <p>Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern. Während der Aktivierung müssen Benutzer ein Mobilgeräteverwaltungsprofil auf ihrem Gerät installieren.</p> <p>Um festzulegen, ob BlackBerry UEM die Aktivierung anhand der Geräte-ID einschränken kann, wählen Sie <b>Nur genehmigte Geräte-IDs zulassen</b> aus.</p>

Aktivierungsart	Beschreibung
Privatsphäre des Benutzers	<p>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.</p> <p><b>Hinweis:</b> 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).</p> <p>Diese Aktivierungsart wird für Apple TV-Geräte nicht unterstützt.</p> <p>Wenn Sie Privatsphäre des Benutzers-Aktivierungen im iOS-Aktivierungsprofil 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:</p> <ul style="list-style-type: none"> <li>• <b>Zugriff auf SIM-Karten- und Geräte-Hardwareinformationen zulassen, um die SIM-basierte Lizenzierung zu aktivieren:</b> Mit dieser Option wird festgelegt, ob BlackBerry UEM auf SIM-Karten- und Geräte-Hardwareinformationen wie ICCID und IMEI zugreifen kann, um zu überprüfen, ob eine entsprechende SIM-Lizenz verfügbar ist.</li> <li>• <b>App-Verwaltung zulassen:</b> 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.</li> <li>• <b>IT-Richtlinienverwaltung zulassen:</b> 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).</li> <li>• <b>E-Mail-Profilverwaltung zulassen:</b> Mit dieser Option wird festgelegt, ob die E-Mail-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen.</li> <li>• <b>WiFi-Profilverwaltung zulassen:</b> Mit dieser Option wird festgelegt, ob die Wi-Fi-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen.</li> <li>• <b>VPN-Profilverwaltung zulassen:</b> Mit dieser Option wird festgelegt, ob die VPN-Profileinstellungen, die dem Benutzer zugewiesen sind, auf das Gerät angewendet werden sollen.</li> </ul>



Aktivierungsart	Beschreibung
Benutzerdatenschutz - Benutzerregistrierung	<p>Sie können die Aktivierungsart „Benutzerdatenschutz - Benutzerregistrierung“ für iOS- und iPad OS-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-Laufwerk, E-Mails (Anhänge und vollständige E-Mail-Texte), Kalender (Anhänge) und iCloud Keychain-Apps installiert.</p> <p>Diese Aktivierungsart ermöglicht die Verwendung von App-Verwaltung, IT-Richtlinienverwaltung, E-Mail-Profilen Wi-Fi-Profilen und „Per App VPN“.</p> <p>Administratoren können geschäftliche Daten verwalten (z. B. geschäftliche Daten löschen), ohne dass Auswirkungen auf persönliche Daten erfolgen.</p> <p>Diese Aktivierungsart wird auf nicht überwachten iPhone- und iPad-Geräten unterstützt, auf denen iOS bzw. iPad OS 13.1 oder höher ausgeführt wird.</p>
Geräteregistrierung nur für BlackBerry 2FA	<p>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.</p> <p>Wenn ein Gerät aktiviert ist, können Sie begrenzte Geräteinformationen in der Verwaltungskonsole anzeigen. Außerdem können Sie das Gerät über einen Befehl deaktivieren.</p> <p>Diese Aktivierungsart wird nur für Microsoft Active Directory-Benutzer unterstützt.</p> <p>Diese Aktivierungsart wird für Apple TV-Geräte nicht unterstützt.</p> <p>Weitere Informationen <a href="#">finden Sie in der Dokumentation zu BlackBerry 2FA</a>.</p>

## Aktivieren eines iOS-Geräts der Version 12.2 oder höher mit dem Aktivierungstyp „MDM-Steuerelemente“

Diese Schritte gelten für Geräte mit iOS Version 12.2 oder höher, die mit MDM-Steuerelemente aktiviert wurden oder bei denen Benutzerdatenschutz mit MDM-Optionen aktiviert ist.

Während der MDM-Registrierung auf Geräten mit iOS Version 12.2 oder höher müssen Benutzer die App BlackBerry UEM Client verlassen und das MDM-Profil manuell installieren. Diese Schritte sind für frühere Versionen von iOS nicht erforderlich.


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

1. Installieren Sie BlackBerry UEM Client auf dem Gerät. Sie können 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

### QR Code zum Aktivieren des Geräts verwenden

- 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, die Ihnen zugesendet wurde, oder im 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-Geräts vor Version 12.2 mit dem Aktivierungstyp „MDM-Steurelemente“


Senden Sie die folgenden Anweisungen an den Gerätebenutzer, um iOS-Geräte vor Version 12.2 mit MDM-Steurelemente zu aktivieren.

1. Installieren Sie BlackBerry UEM Client auf dem Gerät. Sie können 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

### QR Code zum Aktivieren des Geräts verwenden

- 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, die Ihnen zugesendet wurde, oder im BlackBerry UEM Self-Service.
- c. Tippen Sie auf **Weiter**.

4. Tippen Sie auf **OK**, um das Konfigurationsprofil zu installieren.
5. Folgen Sie den Anweisungen auf dem Bildschirm, um die Aktivierung abzuschließen.
6. Wenn Sie aufgefordert werden, das Kennwort für Ihr E-Mail-Konto oder das Kennwort für Ihr Gerät einzugeben, folgen Sie den Anweisungen auf dem Bildschirm.

**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 iPad OS-Gerät mit Apple-Benutzerregistrierung

Die Apple Benutzerregistrierung wird nur auf Geräten mit iPad und iPad OS 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.
- 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 iOS-Geräte verwalten und überwachen

Wenn 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	<p>Sie können für alle verwalteten Geräte die verfügbaren Betriebssystemaktualisierungen anzeigen. Sie können die Installation eines verfügbaren Updates auf folgenden Geräten erzwingen:</p> <ul style="list-style-type: none"><li>• Überwachte Geräte mit iOS 10.3 oder höher</li><li>• Überwachte DEP-Geräte</li></ul> <p>Weitere Informationen finden Sie in der <a href="#">Dokumentation für Administratoren</a>.</p>
Standorteinstellungen und Verloren-Modus aktivieren	<p>Sie können Standorteinstellungen aktivieren, um iOS-Geräte zu orten. Sie können auch den Verloren-Modus aktivieren, um nach einem verlorenen Gerät zu suchen.</p> <p>Weitere Informationen finden Sie in der <a href="#">Dokumentation für Administratoren</a>.</p>
Aktivierungssperre aktivieren	<p>Wenn die Aktivierungssperre auf iOS-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.</p> <p>So verwalten Sie die Aktivierungssperre in BlackBerry UEM:</p> <ul style="list-style-type: none"><li>• Das Gerät muss überwacht werden.</li><li>• Das Gerät muss ein konfiguriertes iCloud-Konto besitzen.</li><li>• Auf dem Gerät muss „Mein iPhone suchen“ oder „Mein iPad suchen“ aktiviert sein.</li></ul> <p>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.</p> <p>Weitere Informationen finden Sie in der <a href="#">Dokumentation für Administratoren</a>.</p>
Geräteprotokolle auslesen	<p>Sie können zu Überwachungs- und Fehlerbehebungs Zwecken Protokolle von Geräten abrufen.</p> <p>Weitere Informationen finden Sie in der <a href="#">Dokumentation für Administratoren</a>.</p>

Option	Beschreibung
Gerät deaktivieren	<p>Wird ein Gerät durch Sie oder einen Benutzer deaktiviert, so 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.</p> <p>Sie können ein Gerät mit dem Befehl „Alle Gerätedaten löschen“ oder „Nur Geschäftsdaten löschen“ deaktivieren.</p> <p>Benutzer können ein iOS-Gerät deaktivieren, indem sie auf dem Bildschirm „Info“ in der BlackBerry UEM Client-App „Mein Gerät deaktivieren“ auswählen.</p>

## Befehle für iOS-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 <a href="#">Anzeigen und Speichern eines Geräteberichts</a> .	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 <a href="#">Anzeigen der Geräteaktionen</a> .	MDM-Steuerelemente Privatsphäre des Benutzers
Alle Gerätedaten löschen	<p>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.</p> <p>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.</p> <p>Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter <a href="#">Senden eines Stapelbefehls</a>.</p>	MDM-Steuerelemente

Befehl	Beschreibung	Aktivierungsarten
Nur geschäftliche Daten löschen	<p>Mit diesem Befehl werden Geschäftsdaten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, vom Gerät gelöscht.</p> <p>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.</p> <p>Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter <a href="#">Senden eines Stapelbefehls</a>.</p>	MDM-Steuerelemente Privatsphäre des Benutzers
Gerät sperren	<p>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.</p> <p>Wenn Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt.</p> <p>Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.</p>	MDM-Steuerelemente
Kennwort entsperren und löschen	<p>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.</p> <p>Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.</p>	MDM-Steuerelemente
Verloren-Modus aktivieren	<p>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.</p> <p>Nachdem Sie diesen Befehl gesendet haben, können Sie den Standort des Geräts in BlackBerry UEM anzeigen.</p> <p>Dieser Befehl wird nur für überwachte iOS-Geräte unterstützt.</p> <p>Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.</p>	
BlackBerry 2FA deaktivieren	<p>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.</p> <p>Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.</p>	MDM-Steuerelemente

Befehl	Beschreibung	Aktivierungsarten
Betriebssystem aktualisieren	<p>Dieser Befehl erzwingt die Installation eines verfügbaren Betriebssystem-Updates. Wird auf den folgenden Geräten unterstützt:</p> <ul style="list-style-type: none"> <li>überwachte Geräte mit iOS 10.3 oder höher</li> <li>überwachte DEP-Geräte</li> </ul> <p>Weitere Informationen finden Sie unter <a href="#">Aktualisieren des Betriebssystems auf beaufsichtigten iOS-Geräten</a>.</p> <p>Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter <a href="#">Senden eines Stapelbefehls</a>.</p> <p>Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.</p>	MDM-Steuerelemente
Gerät neu starten	<p>Dieser Befehl erzwingt den Neustart von Geräten. Unterstützt auf überwachten iOS-Geräten mit Version 10.3 und höher.</p> <p>Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.</p>	MDM-Steuerelemente
Gerät abschalten	<p>Dieser Befehl erzwingt das Ausschalten von Geräten. Unterstützt auf überwachten iOS-Geräten mit Version 10.3 und höher.</p> <p>Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.</p>	MDM-Steuerelemente
Apps bereinigen	<p>Mit diesem Befehl werden die Daten von allen Microsoft Intune-verwalteten Apps auf dem Gerät bereinigt. Die Apps werden nicht vom Gerät entfernt.</p> <p>Weitere Informationen finden Sie unter <a href="#">Von Microsoft Intune verwaltete Apps löschen</a>.</p>	MDM-Steuerelemente
Gerätedaten aktualisieren	<p>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.</p> <p>Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter <a href="#">Senden eines Stapelbefehls</a>.</p>	MDM-Steuerelemente Privatsphäre des Benutzers



Befehl	Beschreibung	Aktivierungsarten
Gerät entfernen	<p>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.</p> <p>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.</p> <p>Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter <a href="#">Senden eines Stapelbefehls</a>.</p>	<p>MDM-Steuerelemente Privatsphäre des Benutzers</p>

# Rechtliche Hinweise

©2020 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada