BlackBerry UEM

Verwalten von Gerätefunktionen

Verwalten

12.12

Inhalt

Verwalten von Gerätefunktionen und -verhalten

Sie haben mehrere Möglichkeiten, das Verhalten eines Geräts zu steuern. Viele Funktionen können Sie mit Profilen und IT-Richtlinien aktivieren oder einschränken. Sie können auch Befehle an Geräte senden, die verschiedene Aktionen einleiten.

Sie haben die Möglichkeit, Einstellungen für verschiedene Gerätetypen in der gleichen IT-Richtlinie oder dem gleichen Profil festzulegen und die IT-Richtlinie oder das Profil dann Benutzerkonten, Benutzergruppen oder Gerätegruppen zuzuweisen.

Verwalten von Geräten mit IT-Richtlinien

Sie können IT-Richtlinien zum Verhalten der Sicherheit und des Verhaltens von Geräten in Ihrer Organisation verwenden. Eine IT-Richtlinie ist ein Regelsatz, mit dem Funktionen und die Funktionalität von Geräten gesteuert werden. Sie können Regeln für BlackBerry 10-, iOS-, macOS-, Android und Windows-Geräte in derselben IT-Richtlinie konfigurieren. Das Betriebssystem des Geräts bestimmt über die Liste der Funktionen, die mit IT-Richtlinien gesteuert werden können, und die Aktivierungsart des Geräts bestimmt, welche Regeln einer IT-Richtlinie für ein bestimmtes Gerät gelten. Geräte ignorieren Regeln einer IT-Richtlinie, die nicht für sie gelten.

BlackBerry UEM enthält eine Standard-IT-Richtlinie mit vorkonfigurierten Regeln für jeden Gerätetyp. Wenn einem Benutzerkonto, einer Benutzergruppe, der ein Benutzer angehört, oder einer Gerätegruppe, dem die Geräte eines Benutzers angehören, keine IT-Richtlinie zugewiesen ist, sendet BlackBerry UEM die Standard-IT-Richtlinie an die Geräte des Benutzers. BlackBerry UEM sendet automatisch eine IT-Richtlinie an ein Gerät, wenn es von einem Benutzer aktiviert wird, wenn Sie eine zugewiesene IT-Richtlinie aktualisieren oder wenn einem Benutzerkonto oder Gerät eine andere IT-Richtlinie zugewiesen wird.

Lokales BlackBerry UEM wird täglich über Port 3101 mit BlackBerry Infrastructure synchronisiert, um zu bestimmen, ob aktualisierte IT-Richtlinieninformationen verfügbar sind. Wenn aktualisierte IT-Richtlinieninformationen verfügbar sind, werden sie von BlackBerry UEM abgerufen und standardmäßig in der BlackBerry UEM-Datenbank gespeichert. Administratoren mit der Berechtigung „IT-Richtlinien anzeigen“ bzw. „IT-Richtlinien erstellen und bearbeiten“ werden über das Update benachrichtigt, wenn sie sich anmelden. Wenn die Sicherheitsrichtlinie Ihres Unternehmens automatische Updates nicht zulässt, können Sie die automatischen Updates deaktivieren und Updates manuell in BlackBerry UEM importieren. Weitere Informationen finden Sie unter Importieren von Updates für IT-Richtlinien und Gerätemetadaten.

Aktualisierte IT-Richtlinieninformationen werden in UEM Cloud-Instanzen automatisch aktualisiert.

Weitere Informationen zu diesen IT-Richtlinienregeln für jeden Gerätetyp finden Sie in der Richtlinien-Referenztabelle.

Einschränken und Zulassen von Gerätefunktionen

Bei der Konfiguration von IT-Richtlinienregeln können Sie Gerätefunktionen einschränken oder zulassen. Die für jeden Gerätetyp zur Verfügung stehenden IT-Richtlinienregeln sind von Betriebssystem und Version des Geräts sowie von der Aktivierungsart der Geräte abhängig. Je nach Gerätetyp und Aktivierungsart können Sie beispielsweise IT-Richtlinienregeln verwenden, um folgende Aufgaben zu erledigen:

- Durchsetzen von Kennwortanforderungen für das Gerät oder den geschäftlichen Bereich auf einem Gerät
- Verhindern, dass Benutzer Gerätefunktionen wie die Kamera verwenden
- Steuern von Verbindungen über die drahtlose Bluetooth-Technologie
- Steuern der Verfügbarkeit bestimmter Apps
- Durchsetzen von Verschlüsselung und anderen Sicherheitsmerkmalen

Je nach Geräteaktivierungsart können Sie mithilfe von IT-Richtlinienregeln das gesamte Gerät, nur den geschäftlichen Bereich eines Geräts oder beides steuern.

Für Geräte mit Android 8.0 und höher können Sie eine Geräte-Supportmeldung erstellen, die auf dem Gerät für einige Funktionen angezeigt wird, wenn sie von einer IT-Richtlinie deaktiviert werden.

Weitere Informationen zu diesen IT-Richtlinienregeln für jeden Gerätetyp finden Sie in der Richtlinien-Referenztabelle.

Einrichten der Anforderungen für Gerätekennwörter

Anforderungen für Gerätekennwörter können mithilfe von IT-Richtlinienregeln eingerichtet werden. Sie können die Anforderungen für die Kennwortlänge und Komplexität, Kennwortablauf und das Ergebnis bei falschen Kennwortversuchen festlegen. Die folgenden Themen erläutern die Regeln für Kennwörter, die für die verschiedenen Geräte und Aktivierungsarten gelten.

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

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 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 iOS-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.
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.

Regel	Beschreibung
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.

Einrichten der macOS-Kennwortanforderungen

Sie können auswählen, ob Kennwortregeln für macOS-Geräte für das Gerät oder den Benutzer gelten sollen, und ob ein Kennwort erforderlich ist. Wenn ein Kennwort erforderlich ist, können Sie die Anforderungen für das Kennwort festlegen.

Regel	Beschreibung
IT-Richtlinienregelziel	Diese Regel gibt an, ob die IT-Richtlinienregeln für das Kennwort nur für das Konto des zugeordneten Benutzers oder für das gesamte Gerät gelten.
Kennwort für Gerät erforderlich	Legen Sie fest, ob der Benutzer ein Gerätekennwort einrichten muss.
Einfaches Kennwort 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 Kennwort	Legen Sie die Mindestlänge des Kennworts fest.
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 Gerätekennwort maximal verwendet werden darf, bevor es abläuft und der Benutzer ein neues Kennwort festlegen muss.
Maximale Zeit für automatische Sperre	Legen Sie die maximale Anzahl der Minuten für die Benutzerinaktivität fest, bevor das Gerät gesperrt wird. Wenn „Keine“ eingestellt ist, kann der Benutzer einen beliebigen Wert auswählen.
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.

Regel	Beschreibung
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor das Gerät bereinigt wird.

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

Einrichten der Android-Kennwortanforderungen

Es gibt vier Gruppen von IT-Richtlinienregeln für Android-Kennwörter. Welche Regeln Sie verwenden, hängt von der Aktivierungsart des Geräts ab, und davon, ob sie Anforderungen für das Gerätekennwort oder das Kennwort für den geschäftlichen Bereich festlegen.

Aktivierungsart	Unterstützte Kennwortregeln
Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) und Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der globalen Kennwortregeln fest. Verwenden Sie die Kennwortregeln für geschäftliche Profile zum Festlegen der Kennwortanforderungen für das geschäftliche Profil. Bei BlackBerry-Geräten, die von Android unterstützt werden, können Sie unterschiedliche Kennwörter für das geschäftliche Profil und das Gerät erzwingen. Die Knox-Kennwortregeln werden vom Gerät ignoriert. Verwenden Sie ein Konformitätsprofil, um Kennwortanforderungen zu erzwingen.
Nur geschäftlicher Bereich (Android Enterprise)	Legen Sie die Kennwortanforderungen für das Gerät mithilfe der globalen Kennwortregeln fest. Da das Gerät nur einen geschäftlichen Bereich besitzt, ist das Kennwort ebenfalls das Kennwort für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert. Verwenden Sie ein Konformitätsprofil, um Kennwortanforderungen zu erzwingen.
MDM-Steuerelemente	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der globalen Kennwortregeln fest. Alle anderen Kennwortregeln werden vom Gerät ignoriert. Verwenden Sie ein Konformitätsprofil, um Kennwortanforderungen zu erzwingen. **Hinweis:** Die Aktivierungsart MDM-Steuerelemente wird für Geräte mit Android 10 nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community.

Aktivierungsart	Unterstützte Kennwortregeln
MDM-Steuerelemente (Knox MDM)	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der Knox MDM-Kennwortregeln fest. Alle anderen Kennwortregeln werden vom Gerät ignoriert. Verwenden Sie ein Konformitätsprofil, um Kennwortanforderungen zu erzwingen.
Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)	Sie haben keine Kontrolle über das Gerätekennwort. Verwenden Sie die Kennwortregeln für Knox Premium – Workspace zum Festlegen der Kennwortanforderungen für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert. Verwenden Sie ein Konformitätsprofil, um Kennwortanforderungen zu erzwingen. **Hinweis:** Die Samsung Knox-Aktivierungsarten werden in einer zukünftigen Version nicht mehr unterstützt. Geräte, die Knox Platform for Enterprise unterstützen, können über die Android Enterprise-Aktivierungsarten aktiviert werden. Weitere Informationen finden Sie in Artikel 54614 unter https://support.blackberry.com/community.
Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)	Legen Sie die Anforderungen für Gerätekennwörter mithilfe der Knox MDM-Kennwortregeln fest. Verwenden Sie die Kennwortregeln für Knox Premium – Workspace zum Festlegen der Kennwortanforderungen für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert. Verwenden Sie ein Konformitätsprofil, um Kennwortanforderungen zu erzwingen.
Nur geschäftlicher Bereich (Samsung Knox)	Verwenden Sie die Kennwortregeln für Knox Premium – Workspace zum Festlegen der Kennwortanforderungen für den geschäftlichen Bereich. Alle anderen Kennwortregeln werden vom Gerät ignoriert. Verwenden Sie ein Konformitätsprofil, um Kennwortanforderungen zu erzwingen.

Android: Globale Kennwortregeln

Die globalen Kennwortregeln legen die Gerätekennwortanforderungen für Geräte mit den folgenden Aktivierungsarten fest:

- Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)
- Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)
- Nur geschäftlicher Bereich (Android Enterprise)
- MDM-Steuerelemente (ohne Samsung Knox)

Hinweis: Die Aktivierungsart MDM-Steuerelemente wird für Geräte mit Android 10 nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community.

Regel	Beschreibung
Kennwortanforderungen	Legen Sie die Mindestanforderungen für das Kennwort fest. Sie können eine der folgenden Optionen auswählen: • Nicht festgelegt – kein Kennwort erforderlich • Eingabe erforderlich – der Benutzer muss ein Kennwort einrichten, wobei es keine Anforderungen an Länge oder Qualität gibt • Numerisch – das Kennwort muss mindestens eine Zahl enthalten • Alphabetisch – das Kennwort muss mindestens einen Buchstaben enthalten • Alphanumerisch – das Kennwort muss mindestens einen Buchstaben und eine Zahl enthalten • Komplex – Sie können bestimmte Anforderungen bezüglich verschiedener Zeichentypen festlegen
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor das Gerät bereinigt oder deaktiviert wird. Geräte mit der Aktivierungsart „MDM-Steuerelemente“ werden bereinigt. Geräte mit den Aktivierungsarten „Geschäftlich und persönlich – Benutzerdatenschutz“ und „Geschäftlich und persönlich – Benutzerdatenschutz (Premium)“ werden deaktiviert, und das Arbeitsprofil wird entfernt.
Maximale Inaktivitätszeit für Sperre	Legen Sie die maximale Anzahl der Minuten für die Benutzerinaktivität fest, nach deren Ablauf das Gerät und der geschäftliche Bereich gesperrt werden. Auf Android-Geräten mit einem geschäftlichen Profil wird auch der geschäftliche Bereich gesperrt. Benutzer können auf dem Gerät einen kürzeren Zeitraum festlegen. Diese Regel wird ignoriert, wenn kein Kennwort erforderlich ist.
Timeout für Kennwortablauf	Legen Sie fest, wie lange das Kennwort maximal verwendet werden kann. Nachdem die angegebene Zeit verstrichen ist muss der Benutzer ein neues Kennwort festlegen. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Einschränkung für Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter das Gerät maximal prüft, um zu verhindern, dass ein vorheriges numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.
Mindestlänge für Kennwort	Legen Sie die Mindestanzahl der Zeichen für ein numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort fest.
Benötigte Mindestanzahl der Großbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Großbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Kleinbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Kleinbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Buchstaben im Kennwort	Legen Sie die Mindestanzahl der Buchstaben fest, die ein komplexes Kennwort enthalten muss.

Regel	Beschreibung
Mindestanzahl von Nicht-Buchstaben in Kennwort	Legen Sie die Mindestanzahl von nicht alphabetischen Zeichen (Zahlen oder Symbole) fest, die ein komplexes Kennwort enthalten muss.
Erforderliche Mindestanzahl an Ziffern in Kennwort	Legen Sie die Mindestanzahl der Zahlenzeichen fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Symbole im Kennwort	Legen Sie die Mindestanzahl an nicht alphanumerischen Zeichen fest, die ein komplexes Kennwort enthalten muss.

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

Android: Kennwortregeln für geschäftliche Profile

Die Kennwortregeln für geschäftliche Profile legen die Kennwortanforderungen für den geschäftlichen Bereich von Geräten mit den folgenden Aktivierungsarten fest:

- Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)
- Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)

Regel	Beschreibung
Kennwortanforderungen	Geben Sie die Mindestanforderungen für das Kennwort für den geschäftlichen Bereich an. Sie können eine der folgenden Optionen auswählen: • Nicht festgelegt – kein Kennwort erforderlich • Eingabe erforderlich – der Benutzer muss ein Kennwort einrichten, wobei es keine Anforderungen an Länge oder Qualität gibt • Numerisch – das Kennwort muss mindestens eine Zahl enthalten • Alphabetisch – das Kennwort muss mindestens einen Buchstaben enthalten • Alphanumerisch – das Kennwort muss mindestens einen Buchstaben und eine Zahl enthalten • Komplex – Sie können bestimmte Anforderungen bezüglich verschiedener Zeichentypen festlegen • Numerisch komplex – das Kennwort muss Zahlen ohne sich wiederholenden (4444) oder geordneten Zahlenfolgen (1234, 4321, 2468) enthalten • Biometrisch schwach – es ist eine biometrische Erkennungstechnologie mit niedriger Sicherheitsstufe für das Kennwort zulässig. Bei BlackBerry-Geräten mit Android können Sie mithilfe der Regel für BlackBerry-Geräte „Unterschiedliches Kennwort für geschäftlichen Bereich und Gerät erzwingen“ unterschiedliche Kennwörter für den geschäftlichen Bereich und das Gerät erzwingen.
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort für den geschäftlichen Bereich eingeben darf, bevor das Gerät deaktiviert und das geschäftliche Profil entfernt wird.

Regel	Beschreibung
Maximale Inaktivitätszeit für Sperre	Legen Sie die maximal Anzahl der Minuten für die Benutzerinaktivität fest, bevor das Gerät und der geschäftliche Bereich gesperrt werden. Wenn Sie sowohl diese Regel als auch die globale Android-Regel „Maximaler Zeitraum der Inaktivität bis Sperre“ festlegen, werden das Gerät und der geschäftliche Bereich gesperrt, wenn einer der beiden Zeiträume abläuft. Benutzer können auf dem Gerät einen kürzeren Zeitraum festlegen.
Timeout für Kennwortablauf	Legen Sie fest, wie lange das Kennwort für den geschäftlichen Bereich maximal verwendet werden kann. Nachdem die angegebene Zeit verstrichen ist, muss der Benutzer ein neues Kennwort für den geschäftlichen Bereich festlegen. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Einschränkung für Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter für den geschäftlichen Bereich das Gerät maximal prüft, um zu verhindern, dass ein vorheriges numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.
Mindestlänge für Kennwort	Legen Sie die Mindestanzahl der Zeichen für ein numerisches, alphabetisches, alphanumerisches oder komplexes Kennwort für den geschäftlichen Bereich fest.
Benötigte Mindestanzahl der Großbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Großbuchstaben fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Benötigte Mindestanzahl der Kleinbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Kleinbuchstaben fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Benötigte Mindestanzahl der Buchstaben im Kennwort	Legen Sie die Mindestanzahl der Buchstaben fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Mindestanzahl von Nicht-Buchstaben in Kennwort	Legen Sie die Mindestanzahl von nicht alphabetischen Zeichen (Zahlen oder Symbole) fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Erforderliche Mindestanzahl an Ziffern in Kennwort	Legen Sie die Mindestanzahl der Zahlenzeichen fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.
Benötigte Mindestanzahl der Symbole im Kennwort	Legen Sie die Mindestanzahl an nicht alphanumerischen Zeichen fest, die ein komplexes Kennwort für den geschäftlichen Bereich enthalten muss.

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

Android: Knox MDM-Kennwortregeln

Die Knox MDM-Kennwortregeln legen die Gerätekennwortanforderungen für Geräte mit den folgenden Aktivierungsarten fest:

- Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)
- MDM-Steuerelemente (Knox MDM)

Geräte mit diesen Aktivierungsarten erfordern ein Gerätekennwort.

Wenn Sie Geräte mit Android Enterprise-Aktivierungsarten für die Verwendung von Knox Platform for Enterprise durchführen, verwenden Sie die Android Global-Kennwortregeln. Die Samsung Knox-Aktivierungsarten und die IT-Richtlinienregeln von Knox MDM werden in einer zukünftigen Version nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 54614 unter https://support.blackberry.com/community.

Hinweis: Die Aktivierungsart MDM-Steuerelemente wird für Geräte mit Android 10 nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 48386 unter https://support.blackberry.com/community.

Regel	Beschreibung
Kennwortanforderungen	Legen Sie die Mindestanforderungen für das Kennwort fest. Sie können eine der folgenden Optionen auswählen: • Numerisch – das Kennwort muss mindestens eine Zahl enthalten • Alphabetisch – das Kennwort muss mindestens einen Buchstaben enthalten • Alphanumerisch – das Kennwort muss mindestens einen Buchstaben und eine Zahl enthalten • Komplex – Sie können bestimmte Anforderungen bezüglich verschiedener Zeichentypen festlegen
Mindestlänge für Kennwort	Legen Sie die Mindestlänge des Kennworts fest. Das Kennwort muss mindestens aus 4 Zeichen bestehen.
Benötigte Mindestanzahl der Kleinbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Kleinbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Großbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Großbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Erforderliche Mindestanzahl an komplexen Zeichen in Kennwort	Legen Sie die Mindestanzahl von komplexen Zeichen (z. B. Zahlen oder Symbole) fest, die ein komplexes Kennwort enthalten muss. Wenn dieser Wert auf 1 festgelegt wird, ist mindestens eine Zahl erforderlich. Wird ein Wert größer als 1 festgelegt, sind mindestens eine Zahl und ein Symbol erforderlich.
Maximallänge für Zeichenfolge	Legen Sie die maximale Länge einer Buchstabenfolge fest, die in einem numerischen, alphabetischen, alphanumerischen oder komplexen Kennwort zulässig ist. Wenn die Länge einer Buchstabenfolge beispielsweise auf 5 eingestellt wird, ist die Buchstabenfolge "abcde" zulässig, die Buchstabenfolge "abcdef" jedoch nicht. Wenn auf 0 gesetzt, bestehen keine Einschränkungen in Bezug auf die Zahl aufeinanderfolgender Buchstaben.

Regel	Beschreibung
Maximale Inaktivitätszeit für Sperre	Legen Sie den Zeitraum der maximalen Benutzerinaktivität fest, der verstreichen muss, bevor das Gerät gesperrt wird (Tastatursperre). Wenn das Gerät mit mehreren EMM-Lösungen verwaltet wird, wird der niedrigste Wert als Inaktivitätszeitraum verwendet. Ist für das Gerät ein Kennwort konfiguriert, muss der Benutzer zum Entsperren des Geräts das Kennwort eingeben. Mit der Einstellung 0 wird das Gerät nicht aufgrund einer Zeitüberschreitung bei Inaktivität gesperrt.
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor das Gerät bereinigt wird.
Einschränkung für Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter das Gerät maximal prüft, um zu verhindern, dass ein Kennwort erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.
Timeout für Kennwortablauf	Legen Sie fest, wie lange das Gerätekennwort maximal verwendet werden kann. Nachdem die angegebene Zeit verstrichen ist, läuft das Kennwort ab, und der Benutzer muss ein neues Kennwort festlegen. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Sichtbarkeit des Kennworts zulassen	Legen Sie fest, ob das Gerätekennwort bei der Eingabe sichtbar sein soll. Wenn diese Regel nicht ausgewählt ist, kann die Sichtbarkeitseinstellung von Benutzern oder Apps nicht geändert werden.
Authentifizierung per Fingerabdruck zulassen	Legen Sie fest, ob der Benutzer die Fingerabdruck-Authentifizierung verwenden darf.

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

Android: Kennwortregeln für Knox Premium - Workspace

Die Kennwortregeln für Knox Premium - Workspace legen die Kennwortanforderungen für den geschäftlichen Bereich von Geräten mit den folgenden Aktivierungsarten fest:

- Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)
- Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)
- Nur geschäftlicher Bereich (Samsung Knox)

Geräte mit diesen Aktivierungsarten erfordern ein Kennwort für den geschäftlichen Bereich.

Wenn Sie Geräte mit Android Enterprise-Aktivierungsarten zur Verwendung von Knox Platform for Enterprise aktivieren, verwenden Sie die Kennwortregeln für geschäftliche Android-Profile. Die Samsung Knox-Aktivierungsarten und die IT-Richtlinienregeln von Knox Premium werden in einer zukünftigen Version nicht mehr unterstützt. Weitere Informationen finden Sie in Artikel 54614 unter https://support.blackberry.com/community.

Regel	Beschreibung
Kennwortanforderungen	Legen Sie die Mindestanforderungen für das Kennwort fest. Sie können eine der folgenden Optionen auswählen: • Numerisch – das Kennwort muss mindestens eine Zahl enthalten • Numerisch komplex – das Kennwort muss mindestens eine Zahl enthalten, darf aber keine sich wiederholenden (4444) oder geordneten Zahlenfolgen (1234, 4321, 2468) aufweisen. • Alphabetisch – das Kennwort muss mindestens einen Buchstaben enthalten • Alphanumerisch – das Kennwort muss mindestens einen Buchstaben und eine Zahl enthalten • Komplex – Sie können bestimmte Anforderungen bezüglich verschiedener Zeichentypen festlegen
Benötigte Mindestanzahl der Kleinbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Kleinbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Benötigte Mindestanzahl der Großbuchstaben im Kennwort	Legen Sie die Mindestanzahl der Großbuchstaben fest, die ein komplexes Kennwort enthalten muss.
Erforderliche Mindestanzahl an komplexen Zeichen in Kennwort	Legen Sie die Mindestanzahl von komplexen Zeichen (z. B. Zahlen oder Symbole) fest, die ein komplexes Kennwort enthalten muss. Mindestens drei komplexe Zeichen sind erforderlich, einschließlich mindestens einer Zahl und eines Symbols.
Maximallänge für Zeichenfolge	Legen Sie die maximale Länge einer Buchstabenfolge fest, die in einem numerischen, alphabetischen, alphanumerischen oder komplexen Kennwort zulässig ist. Wenn die Länge einer Buchstabenfolge beispielsweise auf 5 eingestellt wird, ist die Buchstabenfolge "abcde" zulässig, die Buchstabenfolge "abcdef" jedoch nicht. Wenn auf 0 gesetzt, bestehen keine Einschränkungen in Bezug auf die Zahl aufeinanderfolgender Buchstaben.
Mindestlänge für Kennwort	Legen Sie die Mindestlänge des Kennworts fest. Wenn Sie einen Wert eingeben, der kleiner ist als die für Knox Workspace erforderliche Mindestlänge, wird die Knox Workspace-Mindestlänge verwendet.
Maximale Inaktivitätszeit für Sperre	Legen Sie fest, wie lange der geschäftliche Bereich maximal inaktiv sein muss, bevor dieser Bereich gesperrt wird. Mit der Einstellung 0 wird der geschäftliche Bereich nicht aufgrund einer Zeitüberschreitung bei Inaktivität gesperrt.
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor der geschäftliche Bereich bereinigt wird. Mit der Einstellung 0 gibt es keine Einschränkungen hinsichtlich der Anzahl falscher Kennworteingabeversuche.
Einschränkung für Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter das Gerät maximal prüft, um zu verhindern, dass ein Kennwort erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.

Regel	Beschreibung
Timeout für Kennwortablauf	Legen Sie fest, wie viele Tage das Kennwort maximal verwendet werden kann. Nachdem die angegebene Anzahl von Tagen verstrichen ist, läuft das Kennwort ab, und der Benutzer muss ein neues Kennwort festlegen. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Mindestanzahl geänderter Zeichen für neue Kennwörter	Legen Sie die Mindestanzahl geänderter Zeichen fest, die ein neues Kennwort im Vergleich zu einem vorherigen Kennwort enthalten muss. Wenn 0 eingestellt ist, gelten keine Einschränkungen.
Anpassungen der Tastatursperre zulassen	Legen Sie fest, ob auf einem Gerät Anpassungen der Tastatursperre verwendet werden können, z. B. über Funktionen wie "Trust Agents". Wenn diese Regel nicht ausgewählt ist, werden Anpassungen der Tastatursperre deaktiviert.
Trust Agents bei Tastatursperre zulassen	Legen Sie fest, ob ein Benutzer den geschäftlichen Bereich 2 Stunden über den Zeitüberschreitungswert bei Inaktivität hinaus entsperrt halten kann. Wenn Sie keinen Timeout-Wert für Inaktivität festlegen, kann der Benutzer diese Aktion standardmäßig ausführen.
Sichtbarkeit des Kennworts zulassen	Legen Sie fest, ob das Gerätekennwort bei der Eingabe sichtbar sein soll. Wenn diese Regel nicht ausgewählt ist, kann die Sichtbarkeitseinstellung von Benutzern oder Apps nicht geändert werden.
Zwei-Faktor-Authentifizierung erzwingen	Legen Sie fest, ob ein Benutzer die Zwei-Faktor-Authentifizierung für den Zugriff auf den geschäftlichen Bereich verwenden muss. Sie können diese Regel beispielsweise verwenden, wenn Sie möchten, dass der Benutzer sich per Fingerabdruck und Kennwort authentifizieren muss.
Authentifizierung per Fingerabdruck zulassen	Legen Sie fest, ob der Benutzer die Fingerabdruck-Authentifizierung für den Zugriff auf den geschäftlichen Bereich verwenden kann.

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

Einrichten der Windows-Kennwortanforderungen

Sie können wählen, ob Windows-Geräte ein Kennwort benötigen. Wenn ein Kennwort erforderlich ist, können Sie die Anforderungen für das Kennwort festlegen.

Regel	Beschreibung
Kennwort für Gerät erforderlich	Legen Sie fest, ob der Benutzer ein Gerätekennwort einrichten muss.
Einfaches Kennwort zulassen	Legen Sie fest, ob das Kennwort aufeinanderfolgende und sich wiederholende Zeichen, wie etwa „DEFG“ oder „3333“, enthalten darf.
Mindestlänge für Kennwort	Legen Sie die Mindestlänge des Kennworts fest. Das Kennwort muss mindestens aus 4 Zeichen bestehen.

Regel	Beschreibung
Aufbau von Kennwörtern	Legen Sie die Komplexität des Kennworts fest. Sie können folgende Optionen wählen: • Alphanumerisch – das Kennwort muss Buchstaben und Zahlen enthalten. • Numerisch – das Kennwort darf nur Zahlen enthalten
Mindestanzahl an Zeichentypen	Geben Sie die Mindestanzahl Zeichentypen an, die ein alphanumerisches Kennwort enthalten muss. Wählen Sie aus den folgenden Optionen aus: **1.** Zahlen sind erforderlich. **2.** Zahlen und Kleinbuchstaben sind erforderlich. **3.** Zahlen, Kleinbuchstaben und Großbuchstaben sind erforderlich. **4.** Zahlen, Kleinbuchstaben, Großbuchstaben und Sonderzeichen sind erforderlich. Die Zeichenanforderungen für Kennwörter auf Computern und Tablets mit Windows 10 sind von der Art des Benutzerkontos, nicht von dieser Einstellung abhängig.
Ablauf des Kennworts	Legen Sie fest, wie viele Tage das Kennwort maximal verwendet werden kann. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter das Gerät maximal prüft, um zu verhindern, dass ein Kennwort erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.
Maximale Anzahl ungültiger Kennworteingaben	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor das Gerät bereinigt wird. Wenn auf 0 gesetzt, wird das Gerät nicht bereinigt, unabhängig davon, wie oft der Benutzer ein falsches Kennwort eingibt. Diese Regel gilt nicht für Geräte, die mehrere Benutzerkonten zulassen, z. B. Windows 10-Computer und -Tablets.
Maximale Inaktivitätszeit für Sperre	Legen Sie den Zeitraum für die Benutzerinaktivität fest, bevor das Gerät gesperrt wird. Wenn auf 0 gesetzt, wird das Gerät nicht automatisch gesperrt.
Rückkehr aus Inaktivität ohne Kennwort zulassen	Legen Sie fest, ob ein Benutzer das Kennwort eingeben muss, wenn die Toleranzfrist für Inaktivität endet. Wenn diese Regel ausgewählt ist, kann der Benutzer die Toleranzfrist für das Kennwort auf dem Gerät festlegen. Diese Regel gilt nicht für Windows 10-Computer und -Tablets.

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

Einrichten der BlackBerry 10-Kennwortanforderungen

Auf BlackBerry 10-Geräten beeinflussen die Kennwortregeln das Kennwort für den geschäftlichen Bereich. „Nur geschäftlicher Bereich“-Geräte müssen über ein Kennwort verfügen, und die Anforderungen für das Kennwort können von Ihnen festgelegt werden.

Sie können wählen, ob „Geschäftlich und persönlich – Unternehmen“ und „Geschäftlich und persönlich – Reguliert„- Geräte ein Kennwort für den geschäftlichen Bereich benötigen. Wenn Kennwörter für den geschäftlichen Bereich erforderlich sind, können Sie die Mindestanforderungen für das Kennwort angeben.

Sie können festlegen, ob ein Gerätekennwort ebenfalls erforderlich ist und angeben, ob Kennwörter für den geschäftlichen Bereich und Gerätekennwörter identisch sein müssen.

Regel	Details
Für den geschäftlichen Bereich ist ein Kennwort erforderlich	Angeben, ob Geräte mit der Aktivierungsart „Geschäftlich und persönlich – Unternehmen“ und „Geschäftlich und persönlich – Reguliert“ ein Kennwort für den geschäftlichen Bereich erfordern. Geräte mit der Aktivierungsart „Nur geschäftlicher Bereich“ müssen über ein Kennwort verfügen.
Mindestlänge für Kennwort	Geben Sie die Mindestlänge des Kennworts für den geschäftlichen Bereich an. Das Kennwort muss mindestens aus 4 Zeichen bestehen.
Minimale Kennwortkomplexität	Geben Sie die minimale Komplexität des Kennworts für den geschäftlichen Bereich an. Sie können eine der folgenden Optionen auswählen: • Keine Einschränkung • Mindestens 1 Buchstabe und 1 Zahl • Mindestens 1 Buchstabe, 1 Zahl und 1 Sonderzeichen • Mindestens 1 Großbuchstabe, 1 Kleinbuchstabe, 1 Zahl und 1 Sonderzeichen • Mindestens 1 Großbuchstabe, 1 Kleinbuchstabe und 1 Zahl
Sicherheits-Timeout	Geben Sie den Zeitraum der Inaktivität an, bevor der geschäftliche Bereich gesperrt wird.
Maximale Kennwortversuche	Legen Sie fest, wie oft der Benutzer ein falsches Kennwort eingeben darf, bevor der geschäftliche Bereich bereinigt wird. Auf Geräten mit der Aktivierungsart „Geschäftlich und persönlich – Unternehmen“ und „Geschäftlich und persönlich – Reguliert“ wird das Gerät bereinigt, wenn für den geschäftlichen Bereich und das Gerät das gleiche Kennwort verwendet wird.
Maximaler Kennwortverlauf	Legen Sie fest, wie viele vorherige Kennwörter das Gerät prüft, um zu verhindern, dass ein Kennwort für den geschäftlichen Bereich erneut verwendet wird. Wird 0 verwendet, prüft das Gerät vorherige Kennwörter nicht.
Maximales Kennwortalter	Legen Sie fest, wie viele Tage das Kennwort für den geschäftlichen Bereich maximal verwendet werden kann. Wenn auf 0 gesetzt, läuft das Kennwort nicht ab.
Kennwort für das gesamte Gerät ist erforderlich	Legen Sie fest, ob Geräte mit „Geschäftlich und persönlich – Unternehmen“ und „Geschäftlich und persönlich – Reguliert“ ein Kennwort für das Gerät und den geschäftlichen Bereich erfordern.
Verhalten des Kennworts für geschäftlichen Bereich und Gerät definieren	Geben Sie an, ob das Kennwort für den geschäftlichen Bereich und das Gerätekennwort eines Gerätes unterschiedlich oder gleich sein müssen, oder ob der Benutzer wählen kann, ob die Kennwörter identisch sind.

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

Erstellen und Verwalten von IT-Richtlinien

Sie können die Standard-IT-Richtlinie verwenden oder benutzerdefinierte IT-Richtlinien erstellen (um beispielsweise IT-Richtlinienregeln für verschiedene Benutzergruppen oder Gerätegruppen in Ihrem Unternehmen festzulegen). Wenn Sie vorhaben, die Standard-IT-Richtlinie zu verwenden, sollten Sie diese überprüfen und bei Bedarf aktualisieren, um sicherzustellen, dass die Regeln die Sicherheitsstandards Ihrer Organisation erfüllen.

Erstellen einer IT-Richtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für die IT-Richtlinie ein.
5. Klicken Sie auf die Registerkarte für jeden Gerätetyp in Ihrer Organisation, und konfigurieren Sie die entsprechenden Werte für die IT-Richtlinien.

   Bewegen Sie den Mauszeiger über den Namen einer Regel, um Hilfetipps anzuzeigen.
6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: IT-Richtlinien einen Rang zuweisen

Kopieren einer IT-Richtlinie

Sie können IT-Richtlinien zur schnellen Erstellung benutzerdefinierter IT-Richtlinien für verschiedene Gruppen in Ihrem Unternehmen kopieren.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie kopieren möchten.
4. Klicken Sie auf .
5. Geben Sie einen Namen und eine Beschreibung für die neue IT-Richtlinie ein.
6. Nehmen Sie die gewünschten Änderungen für jeden Gerätetyp auf der entsprechenden Registerkarte vor.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: IT-Richtlinien einen Rang zuweisen

IT-Richtlinien einen Rang zuweisen

Mithilfe der Rangordnung lässt sich festlegen, welche IT-Richtlinie BlackBerry UEM in den folgenden Szenarien an ein Gerät sendet:

- Ein Benutzer ist Mitglied in mehreren Benutzergruppen, die unterschiedliche IT-Richtlinien aufweisen.
- Ein Gerät ist Mitglied in mehreren Gerätegruppen, die unterschiedliche IT-Richtlinien aufweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Klicken Sie auf .
4. Mit den Pfeiltasten können Sie die IT-Richtlinien in der Rangordnung nach oben oder unten verschieben.
5. Klicken Sie auf **Speichern**.

Anzeigen einer IT-Richtlinie

Sie können die folgenden Informationen zu einer IT-Richtlinie anzeigen:

- IT-Richtlinienregeln, speziell für jeden Gerätetyp
- Liste und Anzahl der Benutzerkonten, denen die IT-Richtlinie zugewiesen ist (direkt und indirekt)
- Liste und Anzahl der Benutzergruppen, denen die IT-Richtlinie zugewiesen ist (direkt)

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie anzeigen möchten.

Ändern einer IT-Richtlinie

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie ändern möchten.
4. Klicken Sie auf .
5. Nehmen Sie die gewünschten Änderungen für jeden Gerätetyp auf der entsprechenden Registerkarte vor.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Ändern Sie bei Bedarf die IT-Richtlinienrangordnung.

Entfernen einer IT-Richtlinie aus den Benutzerkonten oder Benutzergruppen

Wenn eine IT-Richtlinie direkt den Benutzerkonten oder Benutzergruppen zugewiesen wurde, können Sie diese aus den Benutzern oder Gruppen entfernen. Wenn eine IT-Richtlinie indirekt durch die Benutzergruppe zugewiesen ist, können Sie die IT-Richtlinie oder die Benutzerkonten aus der Gruppe entfernen. Wenn Sie eine IT-Richtlinie aus den Benutzergruppen entfernen, wird die IT-Richtlinie aus jedem Benutzer entfernt, der den ausgewählten Gruppen angehört.

Hinweis: Die Standard-IT-Richtlinie kann nur dann aus einem Benutzerkonto entfernt werden, wenn Sie es dem Benutzer direkt zugewiesen haben.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Klicken Sie auf den Namen der IT-Richtlinie, die Sie aus den Benutzerkonten oder Benutzergruppen entfernen möchten.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Entfernen einer IT-Richtlinie von Benutzerkonten	**a.** Klicken Sie auf die Registerkarte **Benutzern zugewiesen**. **b.** Suchen Sie ggf. nach den Benutzerkonten. **c.** Wählen Sie die Benutzerkonten aus, aus denen Sie die IT-Richtlinie entfernen möchten. **d.** Klicken Sie auf .

Aufgabe	Schritte
Entfernen einer IT-Richtlinie von Benutzergruppen	**a.** Klicken Sie auf die Registerkarte **Gruppen zugewiesen**. **b.** Suchen Sie ggf. nach den Benutzergruppen. **c.** Wählen Sie die Benutzergruppen aus, aus denen Sie die IT-Richtlinie entfernen möchten. **d.** Klicken Sie auf .

Löschen einer IT-Richtlinie

Sie können die Standard-IT-Richtlinie nicht löschen. Wenn Sie eine benutzerdefinierte IT-Richtlinie löschen, entfernt BlackBerry UEM die IT-Richtlinie für die Benutzer und deren verknüpften Geräten.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Wählen Sie die Kontrollkästchen der IT-Richtlinien aus, die Sie löschen möchten.
4. Klicken Sie auf .
5. Klicken Sie auf **Löschen**.

IT-Richtlinien exportieren

Sie können IT-Richtlinien als XML-Datei zu Prüfzwecken exportieren.

Hinweis:

Profile, die mit IT-Richtlinien verknüpft sind, werden nicht exportiert.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinien > IT-Richtlinien**.
3. Wählen Sie die Kontrollkästchen der IT-Richtlinien aus, die Sie exportieren möchten.
4. Klicken Sie auf .
5. Klicken Sie auf **Weiter**.
6. Klicken Sie auf **Exportieren**.

So wählt BlackBerry UEM die zuzuweisenden IT-Richtlinien aus

BlackBerry UEM sendet nur eine IT-Richtlinie an ein Gerät und verwendet vordefinierte Regeln, um zu bestimmen, welche IT-Richtlinie einem Benutzer und den Geräten, die der Benutzer aktiviert, zugewiesen werden soll.

Zugewiesen zu	Regeln
Benutzerkonto (Registerkarte „Zusammenfassung“)	1. Eine IT-Richtlinie, die einem Benutzerkonto direkt zugewiesen wurde, hat Vorrang vor einer IT-Richtlinie, die indirekt über die Benutzergruppe zugewiesen wurde. 2. Wenn ein Benutzer Mitglied mehrerer Benutzergruppen mit verschiedenen IT-Richtlinien ist, weist BlackBerry UEM die IT-Richtlinie mit der höchsten Rangordnung zu. 3. Die Standard-IT-Richtlinie wird zugewiesen, wenn einem Benutzerkonto keine IT-Richtlinie direkt oder durch die Mitgliedschaft in einer Benutzergruppe zugewiesen wird.
Gerät (Registerkarte „Gerät anzeigen“)	Standardmäßig erbt ein Gerät die IT-Richtlinie, die BlackBerry UEM dem Benutzer zuweist, der das Gerät aktiviert. Wenn ein Gerät einer Gerätegruppe angehört, gelten die folgenden Regeln: 1. Eine IT-Richtlinie, die einer Gerätegruppe zugewiesen ist, hat Vorrang vor der IT-Richtlinie, die BlackBerry UEM einem Benutzerkonto zuweist. 2. Wenn ein Gerät Mitglied mehrerer Gerätegruppen mit verschiedenen IT-Richtlinien ist, weist BlackBerry UEM die IT-Richtlinie mit der höchsten Rangordnung zu.

BlackBerry UEM muss unter Umständen in Konflikt stehende IT-Richtlinien auflösen, falls Sie eine der folgenden Aktionen ausführen:

- Zuweisen einer IT-Richtlinie zu einem Benutzerkonto, einer Benutzergruppe oder einer Gerätegruppe
- Entfernen einer IT-Richtlinie aus einem Benutzerkonto, einer Benutzergruppe oder einer Gerätegruppe
- Ändern der Rangordnung der IT-Richtlinien
- Löschen einer IT-Richtlinie
- Ändern der Zugehörigkeit in einer Benutzergruppe (Benutzerkonten und verschachtelte Gruppen)
- Ändern von Geräteattributen
- Ändern der Mitgliedschaft in einer Gerätegruppe
- Löschen einer Benutzergruppe oder Gerätegruppe

Zulassen, dass BlackBerry 10-Benutzern Gerätedaten sichern

Sie können steuern, ob BlackBerry 10-Benutzer Gerätedaten sichern und wiederherstellen können. Sie können zulassen, dass Benutzer nur Daten aus dem persönlichen Bereich oder Daten sowohl aus dem persönlichen als auch aus geschäftlichen Bereichen sichern können. In der IT-Richtlinie, die Sie Benutzern zuweisen, können Sie eine oder beide der folgenden IT-Richtlinienregeln auswählen:

IT-Richtlinienregel	Anwendbare Aktivierungsarten
Sichern und Wiederherstellen des Geräts zulassen	• Geschäftlich und persönlich – Reguliert • Nur geschäftlicher Bereich

IT-Richtlinienregel	Anwendbare Aktivierungsarten
Sichern und Wiederherstellen des geschäftlichen Bereichs zulassen	• Geschäftlich und persönlich – Unternehmen • Geschäftlich und persönlich – Reguliert **Hinweis:** Für Geräte, die mit „Geschäftlich und persönlich – Reguliert“ aktiviert sind, wird diese Regel nur dann angewendet, wenn die Regel „Sichern und Wiederherstellen des Geräts zulassen“ aktiviert ist.

Wenn die den Benutzern zugewiesene IT-Richtlinie die Gerätesicherung zulässt, können Benutzer sich bei BlackBerry Link anmelden, um Sicherungsdateien zu erstellen oder wiederherzustellen.

Wenn Benutzer Sicherungsdateien mithilfe von BlackBerry Link erstellen, werden die Dateien mithilfe der Verschlüsselungsschlüssel verschlüsselt, die BlackBerry UEM an BlackBerry 10-Geräte sendet. Die ersten Verschlüsselungsschlüssel werden bei der Installation oder einem Upgrade auf BlackBerry UEM Version 12.4 erzeugt. Wenn nötig, können Sie neue Verschlüsselungsschlüssel generieren, Verschlüsselungsschlüssel aus einer anderen BlackBerry UEM-Instanz importieren oder Verschlüsselungsschlüssel exportieren.

Generieren von Verschlüsselungsschlüsseln

Sie können die Verschlüsselungsschlüssel generieren, die zum Verschlüsseln der Sicherungsdateien verwendet werden, wenn Benutzer Daten von BlackBerry 10-Geräten sichern.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > BB10 – Sichern und Wiederherstellen**.
2. Klicken Sie auf **Neuen Schlüssel generieren**.
3. Klicken Sie auf **Erstellen**.

Wenn Sie fertig sind: Die Verschlüsselungsschlüssel werden an alle BlackBerry 10-Geräte gesendet, die in BlackBerry UEM aktiviert sind.

Exportieren von Verschlüsselungsschlüsseln

Sie können Verschlüsselungsschlüssel aus BlackBerry UEM exportieren und die Schlüssel in eine andere BlackBerry UEM-Instanz importieren.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > BB10 – Sichern und Wiederherstellen**.
2. Klicken Sie auf **Schlüssel exportieren**.
3. Geben Sie ein Kennwort ein, und bestätigen Sie es.
4. Klicken Sie auf **Exportieren**.
5. Speichern Sie die Datei.

Importieren von Verschlüsselungsschlüsseln

Sie können Verschlüsselungsschlüssel in BlackBerry UEM importieren, die in einer anderen BlackBerry UEM-Instanz generiert und aus dieser exportiert wurden.

Bevor Sie beginnen: Vergewissern Sie sich, dass Sie über das Kennwort für die Verschlüsselungsschlüsseldatei verfügen, die Sie importieren.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > BB10 – Sichern und Wiederherstellen**.
2. Klicken Sie auf **Schlüssel importieren**.
3. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu der Verschlüsselungsdatei. Klicken Sie auf **Öffnen**.

4. Geben Sie das Kennwort für die Datei ein.
5. Klicken Sie auf **Importieren**.

Entfernen von Verschlüsselungsschlüsseln

Wenn Sie einen neuen Verschlüsselungsschlüssel erstellen, dienen alle zuvor generierten Schlüssel nur noch der Entschlüsselung. Wenn Sie die zuvor generierten Schlüssel nicht mehr benötigen, können Sie sie aus BlackBerry UEM entfernen. Der neueste generierte Verschlüsselungsschlüssel kann nicht entfernt werden.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > BB10 – Sichern und Wiederherstellen**.
2. Um einen Entschlüsselungsschlüssel zu entfernen, klicken Sie neben dem Schlüssel auf ✕.
3. Um zu bestätigen, dass Sie den Schlüssel dauerhaft entfernen möchten, geben Sie „blackberry“ ein. Klicken Sie anschließend auf **Entfernen**.

Importieren von Updates für IT-Richtlinien und Gerätemetadaten

BlackBerry sendet regelmäßig Updates für IT-Richtlinien und Gerätemetadaten an BlackBerry UEM-Installationen, um Informationen zu Updates von Geräte- und Betriebssystemherstellern bereitzustellen.

Wenn beispielsweise ein Gerätehersteller ein neues Gerätemodell veröffentlicht, kann BlackBerry aktualisierte Gerätemetadaten an BlackBerry UEM-Installationen senden, sodass Aktivierungs- und Kompatibilitätsprofile das neue Gerätemodell enthalten und vom Profil zugelassen oder eingeschränkt werden können. Nach der Freigabe von Apple-, Google oder Microsoft-Betriebssystemupdates, kann ein neues IT-Richtlinienpaket an BlackBerry UEM UEM-Installationen gesendet werden, damit Sie die neuen Funktionen im Betriebssystemupdate steuern können.

BlackBerry UEM installiert diese Updates standardmäßig automatisch. Wenn die Sicherheitsrichtlinie Ihres Unternehmens automatische Updates nicht zulässt, können Sie die automatischen Updates deaktivieren und Updates manuell in BlackBerry UEM importieren.

Sie können auch Ereignisbenachrichtigungen einrichten, um Administratoren darüber zu informieren, wenn Updates für IT-Richtlinien und Gerätemetadaten installiert wurden.

Manuelles Importieren von Updates für IT-Richtlinien und Gerätemetadaten

BlackBerry sendet Benachrichtigungen, wenn neue Updates verfügbar sind. Aktualisierungsdateien sind kumulativ. Wenn Sie ein Update verpassen, werden mit dem nächsten Update alle zuvor aktualisierten IT-Richtlinienregeln oder Gerätemetadaten installiert.

Bevor Sie beginnen: Laden Sie die Metadaten oder das IT-Richtlinienpaket gemäß den Anweisungen in der E-Mail-Benachrichtigung herunter.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie auf **Infrastruktur > Konfigurationsdaten importieren**.
3. Führen Sie eine oder beide der folgenden Aktionen aus:
   - Um die automatischen Updates für IT-Richtlinienpakete zu deaktivieren, deaktivieren Sie das Kontrollkästchen **IT-Richtlinienpaketdaten automatisch aktualisieren**.
   - Um die automatischen Updates für Gerätemetadaten zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Gerätemetadaten automatisch aktualisieren**.
4. Klicken Sie auf die entsprechende Schaltfläche **Durchsuchen**, um die Datendatei zu suchen, die Sie importieren möchten. Klicken Sie anschließend auf **Öffnen**.

Erstellen von Geräte-Supportmeldungen

Für Geräte mit Android 8.0 und höher können Sie eine Supportmeldung erstellen, die auf dem Gerät angezeigt wird, wenn eine Funktion von einer IT-Richtlinie deaktiviert wird. Die Meldung wird auf dem Bildschirm „Einstellungen“ der Funktion angezeigt, die deaktiviert ist. Wenn Sie keine Supportmeldung erstellen, zeigt das Gerät die Standardmeldung für das Betriebssystem an.

Sie können auch eine Administrator-Supportmeldung angeben, die auf dem Einstellungsbildschirm der Geräteadministratoren angezeigt wird. Zum Beispiel möchten Sie vielleicht einen Haftungsausschluss anzeigen, der besagt, dass Ihr Unternehmen Apps und Daten im geschäftlichen Profil überwachen und verwalten kann.

Wenn Ihr Unternehmen Benutzer umfasst, die in mehr als einer Sprache arbeiten, können Sie Supportmeldungen in zusätzlichen Sprachen hinzufügen und die Standardsprache angeben, die auf Geräten angezeigt wird, die keine der verfügbaren Sprachen verwenden.

Geräte-Supportmeldungen erstellen

Geräte-Supportmeldungen werden von Geräten mit Android 8.0 und höher unterstützt.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen**.
2. Klicken Sie auf **Benutzerdefinierte Geräte-Supportmeldungen**.
3. Klicken Sie auf der Registerkarte **Benutzerdefinierte Geräte-Supportmeldungen** auf **Hinzufügen**.
4. Wählen Sie die Sprache aus, in der die Benachrichtigung angezeigt werden soll.
5. Geben Sie im Feld **Hinweis zu deaktivierten Funktionen** die Mitteilung ein, die auf dem Gerät angezeigt werden soll, wenn eine Funktion deaktiviert ist. Die Nachricht kann aus bis zu 200 Zeichen bestehen.
6. Optional können Sie im Feld **Administrator-Supportmeldung** einen Hinweis eingeben, der auf dem Einstellungsbildschirm des Geräteadministrators angezeigt wird.
7. Wenn Sie eine Nachricht in mehr als einer Sprache erstellen möchten, klicken Sie auf **Eine weitere Sprache hinzufügen**, und wiederholen Sie die Schritte 4 bis 6 für jede Sprache.
8. Wenn Sie Nachrichten in mehr als einer Sprache hinzugefügt haben, wählen Sie **Standardsprache** neben der Sprache aus, die auf Geräten angezeigt werden soll, die keine der verfügbaren Sprachen verwenden. Wenn beispielsweise Englisch und Französisch die verfügbaren Sprachen sind und Englisch die Standardsprache ist, wird auf Geräten, auf denen Deutsch verwendet wird, die englische Meldung angezeigt.
9. Klicken Sie auf **Speichern**.

Durchsetzen von Kompatibilitätsregeln für Geräte

Sie können Kompatibilitätsprofile verwenden, um Benutzer bei der Einhaltung von Standards Ihres Unternehmens in Bezug auf die Verwendung von Geräten zu unterstützen. Ein Kompatibilitätsprofil definiert die Gerätebedingungen, die in Ihrer Organisation nicht akzeptabel sind. Sie können beispielsweise festlegen, dass Geräte, die entsperrt oder gehackt sind oder für die aufgrund eines nicht autorisierten Zugriffs auf das Betriebssystem ein Integritätsalarm vorliegt, nicht zulässig sind.

Ein Kompatibilitätsprofil legt die folgenden Informationen fest:

- Bedingungen, aufgrund derer ein Gerät nicht kompatibel ist
- E-Mails und Gerätebenachrichtigungen, die von Benutzern empfangen werden, wenn sie gegen die Kompatibilitätsbedingungen verstoßen
- Aktion, die vorgenommen werden, wenn Benutzer das Problem nicht beheben, einschließlich der Einschränkung des Benutzerzugriffs auf die Ressourcen der Organisation, Löschen geschäftlicher Daten auf dem Gerät oder Löschen aller Daten auf dem Gerät

Bei Samsung Knox-Geräten, können Sie eine Liste der gesperrten Apps zu einem Compliance-Profil hinzufügen. BlackBerry UEM setzt jedoch nicht die Kompatibilitätsregeln durch. Stattdessen wird die Liste mit den gesperrten Apps an die Geräte gesendet, die daraufhin die Einhaltung erzwingen. Gesperrte Apps können nicht installiert werden, und wenn sie bereits installiert sind, werden sie deaktiviert. Wenn Sie eine App aus der Liste der gesperrten Apps entfernen, wird die App erneut aktiviert (sofern sie bereits installiert ist).

BlackBerry UEM enthält ein Standard-Konformitätsprofil. Das Standard-Kompatibilitätsprofil setzt keine Kompatibilitätsbedingungen durch. Um Kompatibilitätsregeln durchzusetzen, können Sie die Einstellungen des Standard-Kompatibilitätsprofils ändern oder benutzerdefinierte Kompatibilitätsprofile erstellen und zuweisen. Benutzerkonten, denen kein benutzerdefiniertes Kompatibilitätsprofil zugewiesen wird, wird das Standard-Kompatibilitätsprofil zugewiesen.

Erstellen eines Kompatibilitätsprofils

Bevor Sie beginnen:

- Wenn Sie Regeln zum Sperren oder Zulassen bestimmter Apps definieren, fügen Sie die jeweiligen Apps der Liste der gesperrten Apps hinzu. Weitere Informationen finden Sie unter Hinzufügen einer App zur Liste der gesperrten Apps. Beachten Sie, dass dieser Schritt nicht für integrierte Apps auf überwachten iOS-Geräten gilt. Um integrierte Apps zu sperren, müssen Sie ein Konformitätsprofil erstellen und die Apps zur Liste mit gesperrten Apps hinzufügen. Weitere Informationen finden Sie unter iOS: Kompatibilitätsprofil-Einstellungen.
- Wenn Sie eine E-Mail-Benachrichtigung an Benutzer senden möchten, deren Geräte nicht konform sind, bearbeiten Sie die Standard-E-Mail für Konformitätsverstöße, oder erstellen Sie eine neue E-Mail-Vorlage. Weitere Informationen finden Sie unter Erstellen einer Vorlage für E-Mail-Benachrichtigungen zur Vorschrifteneinhaltung.

Hinweis: Wenn Sie Regeln für gerootete Betriebssysteme, unzulässige Betriebssystemversionen oder unzulässige Gerätemodelle definiert haben, können Benutzer keine neuen Aktivierungen für Geräte abschließen, die nicht regelkonform sind, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Konformität > Konformität**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Kompatibilitätsprofil ein.
5. Wenn Sie Benutzern bei einem nicht konformen Gerät eine Benachrichtigung senden möchten, führen Sie eine der folgenden Aktionen aus:

- Wählen Sie in der Dropdown-Liste **Gesendete E-Mail bei Erkennung einer Verletzung** eine E-Mail-Vorlage aus. Zum Anzeigen der Standard-E-Mail für Konformitätsverstöße klicken Sie auf „Einstellungen > Allgemeine Einstellungen > E-Mail-Vorlagen“.
- Wählen Sie in der Dropdown-Liste **Erzwingungsintervall** aus, wie oft BlackBerry UEM die Konformität überprüft.
- Erweitern Sie **Gesendete Gerätebenachrichtigung bei Erkennung einer Verletzung**. Bearbeiten Sie die Nachricht bei Bedarf.

  Sie können Variablen zum Ausfüllen von Benachrichtigungen mit Benutzer-, Geräte- und Konformitätsinformationen verwenden. Weitere Informationen finden Sie unter Variablen.

6. Klicken Sie auf die Registerkarte für jeden Gerätetyp in Ihrer Organisation, und konfigurieren Sie die entsprechenden Werte für jede Profileinstellung. Weitere Einzelheiten zu den Profileinstellungen finden Sie unter Einstellungen für Kompatibilitätsprofile.
7. Klicken Sie auf **Hinzufügen**.

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

Einstellungen für Kompatibilitätsprofile

Kompatibilitätsprofile werden auf den folgenden Gerätetypen unterstützt:

- BlackBerry 10
- iOS
- macOS
- Android
- Windows

Allgemein: Einstellungen für Kompatibilitätsprofil

Für jede ausgewählte Kompatibilitätsregel wählen Sie auf den Geräte-Registerkarten die Aktion, die BlackBerry UEM durchführen soll, wenn das Gerät eines Benutzers nicht kompatibel ist:

Allgemein: Einstellung für Kompatibilitätsprofil	Beschreibung
Erzwingungsaktion	Diese Einstellung gibt die Aktion an, die BlackBerry UEM auf Geräten durchführt, die nicht kompatibel sind. Mögliche Werte: • Kompatibilitätsprüfung fordern • Nicht vertrauen: Auf iOS-, macOS-, Android- und Windows-Geräten verhindert diese Option, dass der Benutzer auf geschäftliche Ressourcen und Anwendungen vom Gerät zugreift. Daten und Apps werden nicht vom Gerät gelöscht. **Hinweis:** Die Option „nicht vertrauen“ wird für BlackBerry Dynamics-Apps nicht unterstützt. **Hinweis:** Auf iOS-Geräten wird das geschäftliche E-Mail-Konto von der systemeigenen E-Mail-App entfernt. Der Benutzer muss die E-Mail-Konto-Einstellungen in der App wiederherstellen, nachdem die Konformität des Geräts wiederhergestellt wurde. • Quarantäne: Auf BlackBerry 10-Geräten verhindert diese Option, dass der Benutzer auf geschäftliche Ressourcen und Anwendungen vom Gerät zugreift. Daten und Anwendungen werden nicht vom Gerät gelöscht. • Nur geschäftliche Daten löschen • Alle Daten löschen • Vom Server entfernen: Auf BlackBerry 10-, iOS-, Android- und Windows-Geräten kann ein Gerät über BlackBerry UEM deaktiviert werden, wenn es gegen die Regel „Ohne Kontakt“ verstößt. • Keine: Ermöglicht, dass ein Konformitätsverstoß identifiziert, aber keine Maßnahme ergriffen wird. Der Standardwert lautet „Kompatibilitätsprüfung fordern“. Auf Geräten mit Aktivierungsart „Geschäftlich und persönlich – Benutzer-Datenschutz“ können Sie nicht alle Daten auf einem Gerät löschen. Wenn Sie „Alle Daten löschen“ auswählen, führt BlackBerry UEM die gleiche Aktion wie bei „Nur Geschäftsdaten löschen“ aus. Auf Samsung Knox Workspace-Geräten, die nur über einen geschäftlichen Bereich verfügen, werden bei Auswahl der Option „Nur Geschäftsdaten löschen“, „Alle Daten löschen“ oder „Von Server entfernen“ alle Daten vom Gerät gelöscht. Bei iOS-Geräten unter Aufsicht gelten keine Erzwingungsaktionen für die Regel „Eine gesperrte App wurde installiert“. Es wird automatisch verhindert, dass Benutzer gesperrte Apps installieren.

Allgemein: Einstellung für Kompatibilitätsprofil	Beschreibung
Aufforderungsmethode	Die möglichen Werte sind: • Beide • E-Mail-Benachrichtigung • Gerätebenachrichtigung Der Standardwert ist „Beide“. Diese Einstellung gilt nur, wenn die „Erzwingungsaktion“ auf „Kompatibilitätsprüfung fordern“ festgelegt ist. Gerätebenachrichtigungen werden auf Windows 10-Geräten nicht unterstützt.
Anzahl der Aufforderungen	Die Anzahl an Aufforderungen des Benutzers, die Erzwingungsverletzung zu korrigieren. Der Standardwert ist „3“. Diese Einstellung gilt nur, wenn die „Erzwingungsaktion“ auf „Kompatibilitätsprüfung fordern“ festgelegt ist.
Aufforderungsintervall	Die Zeitspanne zwischen Aufforderungen in Minuten, Stunden oder Tagen. Der Standardwert ist „4 Stunden“. Diese Einstellung gilt nur, wenn die „Erzwingungsaktion“ auf „Kompatibilitätsprüfung fordern“ festgelegt ist.
Aktion bei Ablauf des Aufforderungsintervalls	Diese Einstellung definiert, was passiert, wenn der Benutzer die Gesamtzahl an Aufforderungen gemäß „Anzahl der Aufforderungen“ erreicht hat und die Erzwingungsverletzung nicht korrigiert. Mögliche Werte: • Keine • Nicht vertrauen: Auf iOS-, macOS-, Android- und Windows-Geräten verhindert diese Option, dass der Benutzer auf geschäftliche Ressourcen und Anwendungen vom Gerät zugreift. Daten und Anwendungen werden nicht vom Gerät gelöscht. **Hinweis:** Die Option „nicht vertrauen“ wird für BlackBerry Dynamics-Apps nicht unterstützt. Verwenden Sie eine alternative Erzwingungsaktion. • Quarantäne: Auf BlackBerry 10-Geräten verhindert diese Option, dass der Benutzer auf geschäftliche Ressourcen und Anwendungen vom Gerät zugreift. Daten und Anwendungen werden nicht vom Gerät gelöscht. • Nur geschäftliche Daten löschen • Alle Daten löschen Der Standardwert ist „Nicht vertrauen“. Diese Einstellung gilt nur, wenn die „Erzwingungsaktion“ auf „Kompatibilitätsprüfung fordern“ festgelegt ist.

Allgemein: Einstellung für Kompatibilitätsprofil	Beschreibung
Erzwingungsaktion für BlackBerry Dynamics-Apps	Diese Einstellung definiert, was mit BlackBerry Dynamics-Apps geschieht, wenn ein Gerät nicht kompatibel ist. Mögliche Werte: • BlackBerry Dynamics-App-Daten löschen • Ausführen von BlackBerry Dynamics-Apps nicht zulassen Die Standardeinstellung ist „BlackBerry Dynamics-App-Daten löschen“.

iOS: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der möglichen Maßnahmen, wenn Sie eine Kompatibilitätsregel auswählen.

iOS: Kompatibilitätsprofil-Einstellung	Beschreibung
Betriebssystem mit Jailbreak	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass iOS-Geräte nicht gerootet werden. Ein Gerät ist entsperrt (Jailbreak), wenn ein Benutzer oder Angreifer die verschiedenen Einschränkungen auf einem Gerät umgeht, um das Betriebssystem zu ändern. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für gerootete Geräte durchführen, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.
Eine nicht zugewiesene App wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten keine Apps installiert sind, die nicht vom Benutzer zugewiesen wurden. Wenn Sie diese Einstellung auswählen und eine nicht zugewiesene App auf einem iOS-Gerät installiert wird, werden eine Warnmeldung und ein Link auf der Registerkarte „Verwaltete Geräte“ angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der Apps angezeigt, die das Gerät in einen nicht richtlinienkonformen Zustand versetzen. Diese Einstellung gilt nicht für Geräte, die mit Aktivierungsart Privatsphäre des Benutzers aktiviert wurden.
Eine erforderliche App wurde nicht installiert.	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass auf Geräten die erforderlichen Apps installiert sind. Wenn Sie diese Einstellung auswählen und eine erforderliche App nicht auf einem iOS-Gerät installiert ist, wird eine Warnmeldung und ein Link auf der Registerkarte „Verwaltete Geräte“ angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der Anwendungen angezeigt, die das Gerät in einen nicht richtlinienkonformen Zustand versetzen.

iOS: Kompatibilitätsprofil-Einstellung	Beschreibung
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten gemäß dieser Einstellung keine gesperrte Betriebssystemversion installiert ist. Sie können die gesperrten Betriebssystemversionen auswählen. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für Geräte durchführen, die nicht richtlinienkonform sind, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.
Gesperrtes Gerätemodell gefunden	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um Gerätemodelle gemäß dieser Einstellung zu sperren. Mögliche Werte: • Ausgewählte Gerätemodelle zulassen • Ausgewählte Gerätemodelle nicht zulassen Sie können die Gerätemodelle auswählen, die zugelassen oder gesperrt sind. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für Geräte durchführen, die nicht richtlinienkonform sind, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.
Gerät ohne Kontakt	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass Geräte nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind.
Letzte Kontaktzeit	Diese Einstellung gibt die Anzahl an Tagen an, die ein Gerät ohne Kontakt zu BlackBerry UEM sein darf. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gerät ohne Kontakt“ ausgewählt wurde.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliotheksversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.
BlackBerry Dynamics-Verbindung überprüfen	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass BlackBerry Dynamics-Apps nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind. Die Erzwingungsaktion wird auf BlackBerry Dynamics-Apps angewendet.
Verbindungsintervall basiert auf Delegierung der App-Authentifizierung	Diese Einstellung gibt an, dass die Verbindungsüberprüfung darauf basiert, wann eine Authentifizierungsdelegierungs-App eine Verbindung zu BlackBerry UEM herstellt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindung überprüfen“ ausgewählt wurde.

iOS: Kompatibilitätsprofil-Einstellung	Beschreibung
Letzte Kontaktzeit	Diese Einstellung gibt die Anzahl an Tagen an, bis das Gerät eine Verbindung zu BlackBerry UEM herstellen muss. Mögliche Werte: • 8 Stunden • 16 Stunden • 1 Tag • 2 Tage • 3 Tage • 7 Tage • 14 Tage • 30 Tage • 60 Tage • 90 Tage • 180 Tage • 365 Tage Der Standardwert ist „2 Tage“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindung überprüfen“ ausgewählt wurde.

iOS: Kompatibilitätsprofil-Einstellung	Beschreibung

Eine gesperrte App wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um Benutzer an der Installation bestimmter Apps zu hindern.
	
	Um Apps zu sperren, führen Sie eine der folgenden Aufgaben aus:
	
	• Wählen Sie eine App aus der Liste der gesperrten Apps aus. Weitere Informationen finden Sie unter Hinzufügen einer App zur Liste gesperrter Apps.
	
	Führen Sie einen der folgenden Schritte aus:
	
	  • Um Apps anhand des App-Namens auszuwählen, klicken Sie auf die Option „Apps aus der App-Liste auswählen“.
	  • Um Apps anhand der App-Paket-ID auszuwählen, klicken Sie auf die Option „App-Paket-ID angeben“. Sie sollten die Paket-ID nicht zum Hinzufügen öffentlicher Apps verwenden. Fügen Sie der Liste der eingeschränkten Apps öffentliche Apps hinzu, und verwenden Sie dann stattdessen die Option „Apps aus der App-Liste auswählen“, um die Apps auszuwählen.
	• Eine integrierte App auswählen (nur iOS-Geräte unter Aufsicht)
	
	Um eine App aus der Liste zu entfernen, klicken Sie neben der App auf ✕.
	
	Wenn Sie diese Einstellung verwenden und eine eingeschränkte App auf einem iOS-Gerät installiert ist, werden eine Warnmeldung und ein Link auf der Registerkarte „Verwaltete Geräte“ angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der Anwendungen angezeigt, die das Gerät in einen nicht richtlinienkonformen Zustand versetzen.
	
	Bei iOS-Geräten unter Aufsicht gelten keine Erzwingungsaktionen für diese Regel. Es wird automatisch verhindert, dass Benutzer gesperrte Apps installieren. Wenn gesperrte Apps (entweder integriert oder vom Benutzer installiert) bereits installiert sind, werden diese Apps automatisch vom Gerät entfernt.

Nur zulässige Apps auf dem Gerät zeigen	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, die eine Liste mit Apps festlegt, die auf den Geräten der Benutzer installiert werden dürfen. Alle anderen Apps sind nicht zulässig. Um bestimmte Apps zuzulassen, führen Sie eine der folgenden Aufgaben aus: • Wählen Sie eine App aus der Liste der gesperrten Apps aus. Weitere Informationen finden Sie unter Hinzufügen einer App zur Liste gesperrter Apps. • Eine integrierte App auswählen Einige Apps sind standardmäßig in der Liste zulässiger Apps enthalten. Um eine App aus der Liste zu entfernen, klicken Sie neben der App auf ✕. Diese Einstellung ist nur für iOS-Geräte unter Aufsicht gültig.

macOS: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der möglichen Maßnahmen, wenn Sie eine Kompatibilitätsregel auswählen.

macOS: Kompatibilitätsprofil-Einstellung	Beschreibung
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten gemäß dieser Einstellung keine gesperrte Betriebssystemversion installiert ist. Sie können die gesperrten Betriebssystemversionen auswählen. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für Geräte abschließen, die nicht richtlinienkonform sind, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.
Gesperrtes Gerätemodell gefunden	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um Gerätemodelle gemäß dieser Einstellung zu sperren. Mögliche Werte: • Ausgewählte Gerätemodelle zulassen • Ausgewählte Gerätemodelle nicht zulassen Sie können die Gerätemodelle auswählen, die zugelassen oder gesperrt sind. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für Geräte abschließen, die nicht richtlinienkonform sind, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliotheksversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.
BlackBerry Dynamics-Verbindung überprüfen	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass BlackBerry Dynamics-Apps nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind. Die Erzwingungsaktion wird auf BlackBerry Dynamics-Apps angewendet.
Verbindungsintervall basiert auf Delegierung der App-Authentifizierung	Diese Einstellung gibt an, dass die Verbindungsüberprüfung darauf basiert, wann eine Authentifizierungsdelegierungs-App eine Verbindung zu BlackBerry UEM herstellt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindung überprüfen“ ausgewählt wurde.

macOS: Kompatibilitätsprofil-Einstellung	Beschreibung
Letzte Kontaktzeit	Diese Einstellung gibt die Anzahl an Tagen an, bis das Gerät eine Verbindung zu BlackBerry UEM herstellen muss. Mögliche Werte: • 8 Stunden • 16 Stunden • 1 Tag • 2 Tage • 3 Tage • 7 Tage • 14 Tage • 30 Tage • 60 Tage • 90 Tage • 180 Tage • 365 Tage Der Standardwert ist „2 Tage“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindung überprüfen“ ausgewählt wurde.

Android: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der möglichen Maßnahmen, wenn Sie eine Kompatibilitätsregel auswählen.

Android: Kompatibilitätsprofil-Einstellung	Beschreibung
Gerootetes Betriebssystem oder Fehler bei Knox-Nachweis	Mit dieser Einstellung wird eine Kompatibilitätsregel für die Aktionen erstellt, die ausgeführt werden, wenn ein Benutzer oder Angreifer Zugriff auf die Root-Ebene eines Android-Geräts erhält. Ein Gerät wird gerootet, wenn ein Benutzer oder Hacker Zugriff auf die Root-Ebene des Android-Betriebssystems erlangt. Diese Regel gilt für den gerooteten Zustand des Geräts, bei dem der UEM Client, BlackBerry Dynamics SDK oder der Knox-Nachweis den Vorgang erkennt. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für gerootete Geräte durchführen, unabhängig von der von Ihnen festgelegten Erzwingungsaktion. Wenn Sie „Debugging für BlackBerry Dynamics-Apps aktivieren“ auswählen, stoppt die BlackBerry Dynamics Runtime BlackBerry Dynamics-Apps, wenn sie ein aktives Debugging-Tool erkennt. Wenn diese Option deaktiviert ist, führt die BlackBerry Dynamics Runtime keine Aktion aus, wenn ein aktives Debugging-Tool erkannt wird.

Android: Kompatibilitätsprofil-Einstellung	Beschreibung
Fehlgeschlagener SafetyNe Nachweis	Mit dieser Einstellung wird eine Kompatibilitätsregel für die Aktionen erstellt, die ausgeführt werden, wenn der SafetyNet-Nachweis bei einem Gerät nicht erbracht werden kann. Wenn Sie SafetyNet-Nachweise verwenden, sendet BlackBerry UEM Anforderungen zum Testen der Authentizität und der Integrität von Android-Geräten und -Apps in der Umgebung Ihres Unternehmens. Damit diese Einstellungen wirksam werden, müssen Sie in der Verwaltungskonsole unter Einstellungen > Nachweis > SafetyNet-Nachweishäufigkeit die SafetyNet-Nachweisfunktion aktivieren. Weitere Informationen zur Konfiguration von SafetyNet-Nachweisen finden Sie unter Verwalten des Nachweises für Android-Geräte und BlackBerry Dynamics-Apps mit SafetyNet .
Eine nicht zugewiesene App wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten keine Apps installiert sind, die nicht vom Benutzer zugewiesen wurden. Wenn Sie diese Einstellung auswählen und eine nicht zugewiesene App auf einem Android-Gerät installiert wird, werden eine Warnmeldung und ein Link auf der Registerkarte „Verwaltete Geräte“ angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der Anwendungen angezeigt, die das Gerät in einen nicht richtlinienkonformen Zustand versetzen. Auf Android Enterprise- und Samsung Knox-Geräten können Benutzer keine nicht zugewiesenen Apps im geschäftlichen Bereich installieren. Die Erzwingungsaktionen gelten nicht. Diese Einstellung gilt nicht für Geräte mit Privatsphäre des Benutzers-Aktivierung.
Eine erforderliche App wurde nicht installiert.	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass auf Geräten die erforderlichen Apps installiert sind. Wenn Sie diese Einstellung auswählen und eine erforderliche App nicht auf einem Android-Gerät installiert ist, wird eine Warnmeldung und ein Link auf der Registerkarte „Verwaltete Geräte“ angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der Anwendungen angezeigt, die das Gerät in einen nicht richtlinienkonformen Zustand versetzen. Für Android Enterprise-Geräte gelten die Erzwingungsaktionen nicht. Auf Samsung Knox-Geräten werden die erforderlichen internen Apps automatisch installiert. Die Erzwingungsaktionen gelten nur für erforderliche öffentliche Apps.

Android: Kompatibilitätsprofil-Einstellung	Beschreibung
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten gemäß dieser Einstellung keine gesperrte Betriebssystemversion installiert ist. Sie können die gesperrten Betriebssystemversionen auswählen. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für Geräte abschließen, die nicht richtlinienkonform sind, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.
Gesperrtes Gerätemodell gefunden	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um Gerätemodelle gemäß dieser Einstellung zu sperren. Mögliche Werte: • Ausgewählte Gerätemodelle zulassen • Ausgewählte Gerätemodelle nicht zulassen Sie können die Gerätemodelle auswählen, die zugelassen oder gesperrt sind. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für Geräte abschließen, die nicht richtlinienkonform sind, unabhängig von der von Ihnen festgelegten Erzwingungsaktion.
Gerät ohne Kontakt	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass Geräte nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind. Das Gerät überprüft die Einhaltung dieser Regel und kann geschäftliche Daten oder alle Daten löschen oder sich selbst aus BlackBerry UEM löschen, wenn es nicht kompatibel ist. **Letzte Kontaktzeit** Diese Einstellung gibt die Anzahl an Tagen an, die ein Gerät ohne Kontakt zu BlackBerry UEM sein darf.

Android: Kompatibilitätsprofil-Einstellung	Beschreibung
Erforderliche Security Patch-Stufe nicht installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten gemäß dieser Einstellung die erforderlichen Security Patches installiert sind. Sie können die Gerätemodelle und Security Patch-Daten angeben. Geräte mit einem Security Patch, dessen Datum dem angegebenen Datum entspricht oder nach diesem liegt, gelten als konform. **Erzwingungsaktion für BlackBerry Dynamics-Apps** Diese Einstellung definiert, was mit BlackBerry Dynamics-Apps geschieht, wenn ein Gerät nicht mit der Security Patch-Stufe kompatibel ist. Mögliche Werte: • Ausführen von BlackBerry Dynamics-Apps nicht zulassen • BlackBerry Dynamics-App-Daten löschen • Überwachen und Protokollieren Der Standardwert lautet „Ausführen von BlackBerry Dynamics-Apps nicht zulassen“. Sofern Sie zuvor ein Kompatibilitätsprofil erstellt haben, für das die Regel „Erforderliche Security Patch-Stufe ist nicht installiert“ aktiviert ist, wird der Wert nach einem Upgrade auf „Überwachen und Protokollieren“ gesetzt. Diese Einstellung ist nur für aktuelle BlackBerry Dynamics-Apps gültig.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliotheksversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.

Android: Kompatibilitätsprofil-Einstellung	Beschreibung
BlackBerry Dynamics-Verbindung überprüfen	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass BlackBerry Dynamics-Apps nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind. Die Erzwingungsaktion wird auf BlackBerry Dynamics-Apps angewendet. **Verbindungsintervall basiert auf Delegierung der App-Authentifizierung** Diese Einstellung gibt an, dass die Verbindungsüberprüfung darauf basiert, wann eine Authentifizierungsdelegierungs-App eine Verbindung zu BlackBerry UEM herstellt. Diese Einstellung gilt nur, wenn ein Authentifikator in einem BlackBerry Dynamics-Profil angegeben ist. **Letzte Kontaktzeit** Diese Einstellung gibt die Anzahl an Tagen an, bis das Gerät eine Verbindung zu BlackBerry UEM herstellen muss. Mögliche Werte: • 8 Stunden • 16 Stunden • 1 Tag • 2 Tage • 3 Tage • 7 Tage • 14 Tage • 30 Tage • 60 Tage • 90 Tage • 180 Tage • 365 Tage **Erzwingungsaktion für BlackBerry Dynamics-Apps** Diese Einstellung definiert, was mit BlackBerry Dynamics-Apps geschieht, wenn ein Gerät nicht kompatibel ist. Mögliche Werte: • Ausführen von BlackBerry Dynamics-Apps nicht zulassen • BlackBerry Dynamics-App-Daten löschen • Überwachen und Protokollieren Der Standardwert ist „Überwachen und Protokollieren“.

Android: Kompatibilitätsprofil-Einstellung	Beschreibung
Eine gesperrte App wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten keine gesperrten Apps installiert werden. Zum Sperren von Apps lesen Sie Hinzufügen einer App zur Liste der gesperrten Apps. Auf Android Enterprise-Geräten können Benutzer keine gesperrten Apps im geschäftlichen Bereich installieren. Die Erzwingungsaktionen gelten nicht. Auf Samsung Knox-Geräten werden gesperrte Apps im geschäftlichen Bereich automatisch deaktiviert. Die Erzwingungsaktionen gelten nicht. Diese Einstellung gilt nicht für Geräte mit Privatsphäre des Benutzers-Aktivierung. Wenn Sie diese Einstellung verwenden und eine eingeschränkte App auf einem Android-Gerät installiert ist, werden eine Warnmeldung und ein Link auf der Registerkarte „Verwaltete Geräte“ angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der Anwendungen angezeigt, die das Gerät in einen nicht richtlinienkonformen Zustand versetzen.
Das Kennwort erfüllt nicht die Komplexitätsanforderunge	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass der Benutzer Kennwörter für das Gerät und den geschäftlichen Bereich festgelegt hat, die die Komplexitätsanforderungen erfüllen, die ihnen in den IT-Unternehmensrichtlinien zugewiesen wurden.

Windows: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der möglichen Maßnahmen, wenn Sie eine Kompatibilitätsregel auswählen.

Windows: Kompatibilitätsprofil-Einstellung	Beschreibung
Eine erforderliche App wurde nicht installiert.	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass auf Geräten die erforderlichen Apps installiert sind. Interne App-Verfügbarkeit kann nicht überwacht werden.
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten gemäß dieser Einstellung keine gesperrte Betriebssystemversion installiert ist. Sie können die gesperrten Betriebssystemversionen auswählen.
Gesperrtes Gerätemodell gefunden	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um Gerätemodelle gemäß dieser Einstellung zu sperren. Mögliche Werte: • Ausgewählte Gerätemodelle zulassen • Ausgewählte Gerätemodelle nicht zulassen Sie können die Gerätemodelle auswählen, die zugelassen oder gesperrt sind.

Windows: Kompatibilitätsprofil-Einstellung	Beschreibung
Gerät ohne Kontakt	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass Geräte nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliotheksversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.
BlackBerry Dynamics-Verbindung überprüfen	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass BlackBerry Dynamics-Apps nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind. Die Erzwingungsaktion wird auf BlackBerry Dynamics-Apps angewendet.
Antivirus-Signatur	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass auf Geräten eine Antivirus-Signatur aktiviert ist.
Antivirus-Status	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass auf Geräten eine Antivirus-Software aktiviert ist. Sie können die zulässigen Anbieter auswählen.
Firewall-Status	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass auf Geräten eine Firewall aktiviert ist.
Verschlüsselungsstatus	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass Geräte eine Verschlüsselung erfordern.
Windows-Updatestatus	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass BlackBerry UEM auf Geräten Windows-Betriebssystem-Updates installieren oder Benutzer über erforderliche Updates informieren darf.
Eine gesperrte App wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten keine gesperrten Apps installiert werden. Zum Sperren von Apps lesen Sie Hinzufügen einer App zur Liste der gesperrten Apps.
Toleranzperiode ist abgelaufen	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn die Toleranzperiode abgelaufen ist.
Attestation Identity Key (AIK) nicht vorhanden	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn kein AIK auf dem Gerät vorhanden ist.
Richtlinie zur Datenausführungsverhinderung ist deaktiviert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn die DEP-Richtlinie auf dem Gerät deaktiviert ist.
BitLocker ist deaktiviert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn BitLocker auf dem Gerät deaktiviert ist.

Windows: Kompatibilitätsprofil-Einstellung	Beschreibung
Sicherer Start ist deaktiviert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn der sichere Start auf dem Gerät deaktiviert ist.
Codeintegrität ist deaktiviert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn Codeintegritätsfunktion auf dem Gerät deaktiviert ist.
Gerät befindet sich im abgesicherten Modus	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn sich das Gerät im abgesicherten Modus befindet.
Gerät befindet sich in Windows-Vorinstallationsumgebung	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn sich das Gerät in der Windows-Vorinstallationsumgebung befindet.
Treiber für Antischadsoftware-Frühstart ist nicht geladen	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn der Treiber für den Antischadsoftware-Frühstart nicht geladen ist.
Der virtuelle sichere Modus (VSM) ist deaktiviert.	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn der virtuelle sichere Modus deaktiviert ist.
Fehlerbehebung beim Start ist aktiviert.	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn die Fehlerbehebung beim Start aktiviert ist.
Fehlerbehebung für Betriebssystemkern ist aktiviert.	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn die Fehlerbehebung für den Betriebssystemkern aktiviert ist.
Testsignierung ist aktiviert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn die Testsignierung aktiviert ist.
Start-Manager-Revisionsliste weist nicht die erwartete Version auf	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn die Start-Manager-Revisionsliste nicht die erwartete Version aufweist.
Codeintegritäts-Revisionsliste weist nicht die erwartete Version auf	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn die Codeintegritäts-Revisionsliste nicht die erwartete Version aufweist.
Hash für Codeintegritäts-Richtlinie ist vorhanden und ist kein zulässiger Wert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn der Hash für die Codeintegritäts-Richtlinie vorhanden ist und kein zulässiger Wert ist.

Windows: Kompatibilitätsprofil-Einstellung	Beschreibung
Hash für Custom Secure Boot-Konfigurationsrichtlinie ist vorhanden und kein zulässiger Wert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn der Hash für die Custom Secure Boot-Konfigurationsrichtlinie vorhanden ist und einen nicht zulässigen Wert aufweist.
PCR-Wert ist kein zulässiger Wert	Mit dieser Einstellung wird eine Konformitätsregel erstellt, um Aktionen anzugeben, die auftreten, wenn der PCR-Wert nicht zulässig ist.

BlackBerry 10: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der möglichen Maßnahmen, wenn Sie eine Kompatibilitätsregel auswählen.

BlackBerry 10: Kompatibilitätsprofil-Einstellung	Beschreibung
Integritätsalarm	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, falls ein Angreifer herausfinden sollte, wie er Root-Zugriff oder heraufgestufte Berechtigungen auf einem BlackBerry 10-Gerät erhalten kann.
Eine gesperrte Softwareversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass Geräte keine gesperrten Softwareversionen verwenden, die einem Profil für Gerätedienstanforderungen angegeben sind. Weitere Informationen finden Sie unter Erstellen eines Profils für Gerätedienstanforderungen für BlackBerry 10-Geräte. Diese Regel gilt nicht für Geräte mit der Aktivierungsart Geschäftlich und persönlich – Unternehmen.
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten gemäß dieser Einstellung keine gesperrte Betriebssystemversion installiert ist. Sie können die gesperrten Betriebssystemversionen festlegen.
Gesperrtes Gerätemodell gefunden	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um Gerätemodelle gemäß dieser Einstellung zu sperren. Mögliche Werte: • Ausgewählte Gerätemodelle zulassen • Ausgewählte Gerätemodelle nicht zulassen Sie können die Gerätemodelle auswählen, die zugelassen oder gesperrt sind.
Gerät ohne Kontakt	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass Geräte nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu BlackBerry UEM sind.

BlackBerry 10: Kompatibilitätsprofil-Einstellung	Beschreibung
Letzte Kontaktzeit	Diese Einstellung gibt die Anzahl an Tagen an, die ein Gerät ohne Kontakt zu BlackBerry UEM sein darf. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gerät ohne Kontakt“ ausgewählt wurde.

Verwalten von BlackBerry Dynamics-Kompatibilitätsprofilen

BlackBerry Dynamics-Kompatibilitätsprofile werden von Good Control importiert, wenn Sie Good Control mit BlackBerry UEM synchronisieren. Sie können BlackBerry Dynamics-Kompatibilitätsprofile nicht bearbeiten, sie können aber als Referenz verwendet werden, wenn Sie neue Kompatibilitätsprofile in BlackBerry UEM erstellen. Benutzer, die einem Kompatibilitätsprofil in Good Control zugewiesen wurden, bleiben nach der Synchronisierung mit BlackBerry UEM weiterhin demselben Profil zugewiesen. Wenn ein Benutzer einem BlackBerry Dynamics-Kompatibilitätsprofil zugewiesen wird, hat das BlackBerry Dynamics-Kompatibilitätsprofil Vorrang vor allen BlackBerry Dynamics-Regeln in den BlackBerry UEM-Kompatibilitätsprofilen, denen ein Benutzer ebenfalls zugewiesen werden kann.

Einstellung	Beschreibung
Betriebssystem mit Jailbreak	Diese Einstellung gibt die auszuführenden Aktionen an, falls ein Benutzer oder Angreifer die verschiedenen Einschränkungen auf einem iOS-Gerät umgeht, um das Betriebssystem zu modifizieren, unzulässige Apps zu installieren oder heraufgestufte Berechtigungen zu erhalten. Außerdem legt sie die auszuführenden Aktionen für BlackBerry Dynamics-Apps fest, wenn ein Betriebssystem mit Jailbreak verwendet wird.
Betriebssystemversion überprüfen	Diese Einstellung gibt die Betriebssystemversionen an, die zulässig und gesperrt sind, und die Aktionen, die für BlackBerry Dynamics-Apps durchgeführt werden, wenn ein gesperrtes Betriebssystem installiert wird.
Hardwaremodell überprüfen	Diese Einstellung gibt die Hardwaremodelle an, die zulässig und gesperrt sind, und die Aktionen, die für BlackBerry Dynamics-Apps durchgeführt werden, wenn ein gesperrtes Hardwaremodell verwendet wird.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Diese Einstellung gibt die BlackBerry Dynamics-Bibliotheken an, die verwendet werden können, sowie die Aktionen, die für BlackBerry Dynamics-Apps durchgeführt werden, wenn ein Gerät mit einer unzulässigen Bibliotheksversion verwendet wird.

Einstellung	Beschreibung
Verbindung überprüfen	Diese Einstellung gibt an, ob ein Gerät innerhalb einer bestimmten Anzahl an Tagen eine Verbindung zu BlackBerry UEM herstellen muss. Außerdem gibt sie die Aktionen an, die für BlackBerry Dynamics-Apps durchgeführt werden, wenn ein Gerät keine Verbindung zu BlackBerry UEM herstellt. Die untergeordnete Einstellung „Verbindungsintervall basiert auf Delegierung der App-Authentifizierung“ gibt an, ob die als Delegierung der Authentifizierung festgelegte App das Verbindungsintervall steuert. Wenn Sie die Delegierung der Authentifizierung zur Verwaltung des Verbindungsintervalls verwenden, werden seltener verwendete Apps nicht gesperrt oder gelöscht, wenn diese keine Verbindung zu BlackBerry UEM herstellen.

Senden von Befehlen an Benutzer und Geräte

Sie können verschiedene Befehle senden, um Benutzerkonten und -geräte zu verwalten. Die Liste der verfügbaren Befehle hängt vom Gerätetyp und von der Aktivierungsart ab. Befehle können an einen bestimmten Benutzer bzw. ein bestimmtes Gerät oder über Stapelbefehle an mehrere Benutzer und Geräte gesendet werden.

Sie können Befehle beispielweise in folgenden Situationen verwenden:

- Wenn ein Gerät vorübergehend verlegt wurde, können Sie einen Befehl zum Sperren des Geräts senden oder geschäftliche Daten auf dem Gerät löschen.
- Wenn Sie ein Gerät einem anderen Benutzer in Ihrem Unternehmen zuteilen möchten oder wenn ein Gerät verloren gegangen ist oder gestohlen wurde, können Sie einen Befehl senden, um alle Daten auf dem Gerät zu löschen.
- Wenn ein Mitarbeiter aus Ihrem Unternehmen ausscheidet, können Sie einen Befehl an das persönliche Gerät des Benutzers senden, um ausschließlich die geschäftlichen Daten zu löschen.
- Wenn ein Benutzer das Kennwort für den geschäftlichen Bereich vergisst, können Sie einen Befehl senden, um dieses Kennwort zurückzusetzen.
- Bei Benutzern mit beaufsichtigten DEP-Geräten können Sie einen Befehl senden, um eine Aktualisierung des Betriebssystems auszulösen.

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 Festlegen einer Ablaufzeit 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.

Senden eines Stapelbefehls

Sie können einen Befehl an mehrere Benutzerkonten oder Geräte gleichzeitig senden, indem Sie die Benutzer bzw. Geräte in der Benutzerliste auswählen und einen Stapelbefehl senden.

Bevor Sie beginnen: Wenn Sie ein Ablaufdatum für Befehle einrichten möchten, mit denen Daten aus Geräten gelöscht werden, lesen Sie den Abschnitt Festlegen einer Ablaufzeit für Befehle.

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Falls erforderlich, können Sie die Benutzerliste filtern.
3. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen oben in der Benutzerliste, um alle Benutzer und Geräte in der Liste auszuwählen.
   - Aktivieren Sie das Kontrollkästchen für alle Benutzer und Geräte, die Sie einbeziehen möchten. Sie können mit Umschalttaste + Mausklick mehrere Benutzer auswählen.
4. Klicken Sie im Menü auf eines der folgenden Symbole:

Symbol	Beschreibung
	Gerätestandorte bestimmen Sie können maximal 100 Geräte gleichzeitig auswählen. Weitere Informationen finden Sie unter Standort eines Geräts bestimmen.
	E-Mail senden Weitere Informationen finden Sie unter Senden einer E-Mail an Benutzer.
	Aktivierungs-E-Mail senden Weitere Informationen finden Sie unter Senden einer Aktivierungs-E-Mail an mehrere Benutzer.
	Zu Benutzergruppen hinzufügen Sie können maximal 200 Geräte gleichzeitig auswählen. Weitere Informationen finden Sie unter Hinzufügen von Benutzern zu Benutzergruppen.
	Exportieren Weitere Informationen finden Sie unter Exportieren der Benutzerliste in eine CSV-Datei.
	Geräte entfernen Sie müssen Sie Sicherheitsadministrator sein, um diesen Stapelbefehl verwenden zu können. Sie können maximal 200 Geräte gleichzeitig auswählen. Weitere Informationen finden Sie unter Befehlsreferenz.
	Geräteinformationen aktualisieren Weitere Informationen finden Sie unter Befehlsreferenz.
	Alle Gerätedaten löschen Sie müssen Sie Sicherheitsadministrator sein, um diesen Befehl verwenden zu können. Sie können maximal 200 Geräte gleichzeitig auswählen. Dieser Stapelbefehl wird für macOS-Geräte nicht unterstützt. Weitere Informationen finden Sie unter Befehlsreferenz.
	Nur geschäftliche Daten löschen Sie müssen Sie Sicherheitsadministrator sein, um diesen Befehl verwenden zu können. Sie können maximal 200 Geräte gleichzeitig auswählen. Weitere Informationen finden Sie unter Befehlsreferenz.

Symbol	Beschreibung
	Geräteeigentümer bearbeiten Sie können maximal 100 Geräte gleichzeitig auswählen. Weitere Informationen finden Sie unter Ändern der Bezeichnung für den Geräteeigentümer.
	Betriebssystem aktualisieren Sie können die Installation eines verfügbaren Betriebssystem-Updates auf beaufsichtigten iOS-Geräten erzwingen: Sie müssen Sie Sicherheitsadministrator sein, um diesen Befehl verwenden zu können. Sie können maximal 200 Geräte gleichzeitig auswählen. Weitere Informationen finden Sie unter Aktualisieren des Betriebssystems auf beaufsichtigten iOS-Geräten.
	Konsolenkennwörter ändern Sie können ein BlackBerry UEM Self-Service-Kennwort an mehrere Benutzer gleichzeitig senden. Weitere Informationen finden Sie unter Senden eines BlackBerry UEM Self-Service-Kennworts an mehrere Benutzer.

Festlegen einer Ablaufzeit für Befehle

Wenn Sie den Befehl „Alle Gerätedaten senden“ oder „Nur geschäftliche Daten löschen“ an ein Gerät senden, muss das Gerät mit BlackBerry UEM verbunden sein, damit der Befehl ausgeführt wird. Wenn das Gerät keine Verbindung zu BlackBerry UEM herstellen kann, bleibt der Befehl im Status „Ausstehend“, und das Gerät wird nicht aus BlackBerry UEM entfernt, es sei denn, Sie entfernen es manuell. Alternativ können Sie BlackBerry UEM so konfigurieren, dass Geräte automatisch entfernt werden, wenn Befehle nach einem bestimmten Zeitraum nicht ausgeführt wurden.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Ablauf des Löschbefehls**.
2. Wählen Sie für die Befehle **Alle Gerätedaten löschen** und **Nur geschäftliche Daten löschen** die Option **Gerät automatisch entfernen, wenn der Befehl nicht abgeschlossen wurde**.
3. Geben Sie im Feld **Ablauf des Befehls** die Anzahl der Tage ein, nach denen der Befehl abläuft und das Gerät automatisch aus BlackBerry UEM entfernt wird.
4. Klicken Sie auf **Speichern**.

Befehlsreferenz

Die Befehle, die Sie an Geräte senden können, hängen vom Gerätetyp und von der Aktivierungsart ab. Einige Befehle können an mehrere Geräte gleichzeitig gesendet werden.

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 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
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

Befehl	Beschreibung	Aktivierungsarten
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. Dieser Befehl wird nur für überwachte iOS-Geräte unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	
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
Betriebssystem aktualisieren	Dieser Befehl erzwingt die Installation eines verfügbaren Betriebssystem-Updates. Wird auf den folgenden Geräten unterstützt: • überwachte Geräte mit iOS 10.3 oder höher • überwachte DEP-Geräte 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. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Gerät neu starten	Dieser Befehl erzwingt den Neustart von Geräten. Unterstützt auf überwachten iOS-Geräten mit Version 10.3 und höher. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Gerät abschalten	Dieser Befehl erzwingt das Ausschalten von Geräten. Unterstützt auf überwachten iOS-Geräten mit Version 10.3 und höher. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente

Befehl	Beschreibung	Aktivierungsarten
Apps bereinigen	Mit diesem Befehl werden die Daten von allen 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
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

Befehle für macOS-Geräte

Befehl	Beschreibung
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.
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.
Desktop sperren	Mit diesem Befehl können Sie eine PIN festlegen und das Gerät sperren.
Nur geschäftliche Daten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht und das Gerät optional aus BlackBerry UEM entfernt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.

Befehl	Beschreibung
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten vom Gerät gelöscht. Das Gerät wird auf die Werkseinstellungen zurückgesetzt, mit einer von Ihnen festgelegten PIN gesperrt und optional aus BlackBerry UEM gelöscht.
Desktopdaten 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.
Gerät entfernen	Dieser Befehl entfernt das Gerät aus BlackBerry UEM. Das Gerät empfängt ggf. weiterhin E-Mails und andere geschäftliche Daten. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.

Befehle für Android-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.	Alle (außer BlackBerry 2FA)
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.	Alle (außer BlackBerry 2FA)
Gerät sperren	Mit diesem Befehl sperren Sie das 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.	MDM-Steuerelemente Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Nur geschäftlicher Bereich (Android Enterprise)

Befehl	Beschreibung	Aktivierungsarten
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind, einschließlich der im geschäftlichen Bereich, und das Gerät wird auf die Werkseinstellungen 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 es entfernt wurde, werden nur die Geschäftsdaten vom Gerät gelöscht. Gegebenenfalls wird auch der geschäftliche Bereich entfernt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)
Nur geschäftliche Daten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht, und das Gerät wird deaktiviert. Wenn das Gerät über einen geschäftlichen Bereich verfügt, werden die Informationen im geschäftlichen Bereich sowie der Bereich selbst vom Gerät gelöscht. Weitere Informationen finden Sie unter Deaktivieren von Geräten. Wenn Sie diesen Befehl auf Android Enterprise Geschäftlich und persönlich – Benutzer-Datenschutz-Geräten verwenden, können Sie einen Grund für das Löschen des geschäftlichen Profils eingeben, der in der Benachrichtigung auf dem Gerät des Benutzers angezeigt wird. 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 es gelöscht wurde, werden die Geschäftsdaten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	MDM-Steuerelemente Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)

Befehl	Beschreibung	Aktivierungsarten
Gerät entsperren und Kennwort löschen	Mit diesem Befehl wird das Gerät gesperrt und der Benutzer zum Erstellen eines neuen Gerätekennworts aufgefordert. Wenn der Benutzer den Bildschirm „Gerätekennwort erstellen“ überspringt, wird das vorherige Kennwort beibehalten. Sie können diesen Befehl verwenden, wenn ein Benutzer sein Gerätekennwort vergessen hat. **Hinweis:** Dieser Befehl wird nicht auf Nicht-Samsung-Geräten nicht unterstützt, die mit MDM-Steuerelemente aktiviert wurden.	MDM-Steuerelemente Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)
Gerätekennwort festlegen und sperren	Mit diesem Befehl können Sie ein Gerätekennwort erstellen und das Gerät anschließend sperren. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Um das Gerät zu entsperren, muss der Benutzer das neue Kennwort eingeben. **Hinweis:** Dieser Befehl wird auf nicht-Samsung-Geräten mit Android 7.0 und höher und der Aktivierungsart MDM-Steuerelemente nicht unterstützt. **Hinweis:** Für die Geschäftlich und persönlich – Benutzer-Datenschutz-Aktivierungsarten unterstützen nur BlackBerry-Geräte mit Android 8.x und höher diesen Befehl.	MDM-Steuerelemente Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Nur geschäftlicher Bereich (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise)
Kennwort für geschäftlichen Bereich zurücksetzen	Dieser Befehl löscht das aktuelle Kennwort für den geschäftlichen Bereich vom Gerät. Wenn der Benutzer den geschäftlichen Bereich öffnet, fordert das Gerät ihn auf, ein neues Kennwort für den geschäftlichen Bereich festzulegen.	Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz - (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)
Geschäftlichen Bereich sperren und Kennwort festlegen	Sie können ein Kennwort für das geschäftliche Profil angeben und das Gerät sperren. Wenn der Benutzer eine geschäftliche App öffnet, muss er das von Ihnen festgelegte Kennwort eingeben.	Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)

Befehl	Beschreibung	Aktivierungsarten
Geschäftlichen Bereich aktivieren/ deaktivieren	Dieser Befehl aktiviert bzw. deaktiviert den Zugriff auf die Apps für den geschäftlichen Bereich auf dem Gerät.	Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz - (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox)
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.	BlackBerry 2FA
Apps bereinigen	Mit diesem Befehl werden die Daten von allen 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.	Alle (außer BlackBerry 2FA)
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.	Alle (außer BlackBerry 2FA)
Fehlerbericht anfordern	Dieser Befehl fordert Client-Protokolle vom Gerät an. Der Gerätebenutzer muss die Anfrage annehmen oder ablehnen.	Nur geschäftlicher Bereich (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)
Gerät neu starten	Dieser Befehl sendet eine Neustart-Anforderung an das Gerät. Dem Benutzer wird eine Meldung angezeigt, dass das Gerät in einer Minute neu gestartet wird. Der Gerätebenutzer kann den Neustart 10 Minuten lang verzögern.	Nur geschäftlicher Bereich (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise)

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.	Alle (außer BlackBerry 2FA)

Befehle für Windows-Geräte

Befehl	Beschreibung
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.
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.
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 nur auf Geräten unterstützt, auf denen Windows 10 Mobile ausgeführt wird.
Gerätekennwort erstellen und Gerät sperren	Mit diesem Befehl wird ein neues Kennwort generiert und das Gerät gesperrt. Das generierte Kennwort wird dem Benutzer per E-Mail gesendet. Sie können die vorgewählte E-Mail-Adresse verwenden oder eine E-Mail-Adresse angeben. Das generierte Kennwort erfüllt alle bestehenden Kennwortregeln. Dieser Befehl wird nur auf Geräten unterstützt, auf denen Windows 10 Mobile ausgeführt wird.

Befehl	Beschreibung
Nur geschäftliche Daten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht und das Gerät optional aus BlackBerry UEM entfernt. Durch Senden dieses Befehls wird das Benutzerkonto nicht gelöscht. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BlackBerry UEM löschen. Wenn das Gerät keine Verbindung zu BlackBerry UEM herstellen kann, können Sie es aus BlackBerry UEM löschen. Wenn das Gerät eine Verbindung zu BlackBerry UEM herstellt, nachdem es entfernt wurde, werden nur die geschäftlichen Daten sowie gegebenenfalls der geschäftliche Bereich vom Gerät gelöscht. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind. Er setzt das Gerät auf die werkseitigen Standardeinstellungen zurück und löscht das Gerät optional aus BlackBerry UEM. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus BlackBerry UEM löschen. Wenn das Gerät keine Verbindung zu BlackBerry UEM herstellen kann, können Sie es aus BlackBerry UEM löschen. Wenn das Gerät eine Verbindung zu BlackBerry UEM herstellt, nachdem es entfernt wurde, werden nur die geschäftlichen Daten sowie gegebenenfalls der geschäftliche Bereich vom Gerät gelöscht. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.
Desktop/Gerät neu starten	Dieser Befehl erzwingt den Neustart von Geräten.
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. Der Befehl sendet zudem eine Anfrage über die Erstellung einer Anfrage auf Überprüfung des Health-Zertifikats an das Gerät. Das Gerät sendet die Anfrage an den Microsoft Health Attestation-Dienst, um die Konformität zu prüfen. Diese Funktion wird nur in einer lokalen Umgebung unterstützt. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.
Gerät entfernen	Dieser Befehl entfernt das Gerät aus BlackBerry UEM. Das Gerät empfängt ggf. weiterhin E-Mails und andere geschäftliche Daten. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.

Befehle für BlackBerry 10-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.	Geschäftlich und persönlich – Unternehmen Nur geschäftlicher Bereich Geschäftlich und persönlich – Reguliert
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.	Geschäftlich und persönlich – Unternehmen Nur geschäftlicher Bereich Geschäftlich und persönlich – Reguliert
Gerätekennwort festlegen, Gerät sperren und Nachricht einrichten	Mit diesem Befehl erstellen Sie ein Gerätekennwort und legen eine Nachricht fest, die auf dem Startbildschirm angezeigt wird. Anschließend wird das Gerät gesperrt. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Wenn der Benutzer das Gerät entsperrt, wird er vom Gerät aufgefordert, das neue Kennwort zu akzeptieren oder abzulehnen. Wenn eine IT-Richtlinie erfordert, dass das Gerät das gleiche Kennwort für das Gerät und den geschäftlichen Bereich nutzen muss, ändert dieser Befehl zudem das Kennwort für den geschäftlichen Bereich.	Geschäftlich und persönlich – Unternehmen Nur geschäftlicher Bereich Geschäftlich und persönlich – Reguliert
Alle Gerätedaten löschen	Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind, einschließlich der im geschäftlichen Bereich. Er setzt das Gerät auf die werkseitigen Standardeinstellungen zurück und löscht das Gerät optional aus BlackBerry UEM. 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.	Geschäftlich und persönlich – Unternehmen Nur geschäftlicher Bereich Geschäftlich und persönlich – Reguliert

Befehl	Beschreibung	Aktivierungsarten
Geschäftlichen Bereich sperren und Kennwort festlegen	Mit diesem Befehl können Sie ein Kennwort für den geschäftlichen Bereich auf dem Gerät festlegen und den geschäftlichen Bereich sperren. Sie müssen ein Kennwort erstellen, das die bestehenden Kennwortregeln erfüllt. Um den geschäftlichen Bereich zu entsperren, muss der Benutzer das neue von Ihnen erstellte Kennwort eingeben. Wenn eine IT-Richtlinie erfordert, dass das Gerät das gleiche Kennwort für das Gerät und den geschäftlichen Bereich nutzen muss, ändert dieser Befehl zudem das Gerätekennwort.	Geschäftlich und persönlich – Unternehmen Geschäftlich und persönlich – Reguliert
Nur geschäftliche Daten löschen	Mit diesem Befehl werden geschäftliche Daten, einschließlich der auf dem Gerät vorhandenen IT-Richtlinie, Profile, Apps und Zertifikate, gelöscht und das Gerät optional aus BlackBerry UEM entfernt. Wenn das Gerät über einen geschäftlichen Bereich verfügt, werden die Informationen im geschäftlichen Bereich sowie der Bereich selbst aus dem 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.	Geschäftlich und persönlich – Unternehmen Geschäftlich und persönlich – Reguliert
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.	Geschäftlich und persönlich – Unternehmen Nur geschäftlicher Bereich Geschäftlich und persönlich – Reguliert
Gerät entfernen	Dieser Befehl entfernt das Gerät aus BlackBerry UEM. Das Gerät empfängt ggf. weiterhin E-Mails und andere geschäftliche Daten. Informationen zum Senden dieses Befehls an mehrere Geräte finden Sie unter Senden eines Stapelbefehls.	Geschäftlich und persönlich – Unternehmen Nur geschäftlicher Bereich Geschäftlich und persönlich – Reguliert

Deaktivieren von Geräten

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.

Sie können ein Gerät mit dem Befehl „Nur Geschäftsdaten löschen“ deaktivieren. BlackBerry UEM kann ein Gerät auch deaktivieren, wenn es gegen das Konformitätsprofil verstößt und die angegebene Erzwingungsaktion darin besteht, das Gerät zu deaktivieren. Benutzer können ihre Geräte mit den folgenden Methoden deaktivieren:

- Benutzer haben die Möglichkeit, für iOS- und Android-Geräte auf dem Bildschirm „Info“ in der BlackBerry UEM Client-App „Mein Gerät deaktivieren“ auszuwählen.
- Für Windows 10-Geräte können Benutzer „Einstellungen > Konten > Geschäftlicher Zugriff > Löschen“ auswählen.
- Für BlackBerry 10-Geräte können die Benutzer „Einstellungen > BlackBerry Balance > Geschäftlichen Bereich löschen“ auswählen.

Wenn bei Geräten, die Knox MDM verwenden, das Gerät deaktiviert wird, werden interne Anwendungen deinstalliert, und die Option „Deinstallieren“ wird für beliebige öffentliche Apps, die von der Apps-Liste aus installiert wurden, nach Bedarf verfügbar.

Für Android Enterprise-Geräte, auf denen nur ein geschäftliches Profil vorliegt, haben Sie bei der Deaktivierung eines Geräts die Möglichkeit, alle Daten von der SD-Karte zu löschen und den werkseitigen Rücksetzschutz aufzuheben.

Auf Android Enterprise-Geräten mit Geschäftlich und persönlich – Benutzer-Datenschutz-Aktivierungen können Sie bei Verwendung des Befehls „Nur Geschäftsdaten löschen“ einen Grund für das Löschen des geschäftlichen Profils eingeben, der in der Benachrichtigung auf dem Gerät des Benutzers angezeigt wird. Wenn das Gerät aufgrund eines Verstoßes gegen die Konformitätsregeln deaktiviert wird, gibt die Benachrichtigung den Grund an, warum das Gerät nicht richtlinienkonform war.

Bei Samsung Knox Workspace-Geräten, die mit den Geschäftlich und persönlich – vollständige Kontrolle- oder Nur geschäftlicher Bereich-Aktivierungsarten aktiviert wurden, führt das Deaktivieren des Geräts dazu, dass alle Daten von dem Gerät oder nur aus dem geschäftlichen Bereich gelöscht werden. Sie können mit der IT-Richtlinienregel „Löschen von Daten bei Deaktivierung“ angeben, welche Daten gelöscht werden.

Steuern der Softwareupdates, die auf Geräten installiert sind

Sie können die Softwareversionen steuern, die auf Android Enterprise-Geräten, Samsung Knox- und BlackBerry 10-Geräten installiert sind. Bei Android Enterprise-Geräten können Sie auch einen Aktualisierungszeitraum für Apps festlegen, die im Vordergrund ausgeführt werden.

Bei Android Enterprise-Geräten mit Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Aktivierungen können Sie festlegen, ob der Benutzer auswählen kann, wann verfügbare Softwareupdates installiert werden sollen oder ob Softwareupdates automatisch installiert werden. Sie können je nach Gerätemodell und aktuell installierter Betriebssystemversion unterschiedliche Regeln festlegen. Bei allen Android Enterprise-Geräten können Sie auch einen Aktualisierungszeitraum für Apps festlegen, die im Vordergrund ausgeführt werden, da Google Play sie standardmäßig nicht aktualisieren kann, wenn eine App im Vordergrund ausgeführt wird. Sie können auch steuern, wie Google Play die Änderungen auf das Gerät anwendet, z. B. indem Sie angeben, ob der Benutzer die Änderung zulassen darf oder ob die Änderung nur dann stattfindet, wenn das Gerät mit einem Wi-Fi-Netzwerk verbunden ist.

Auf Samsung Knox-Geräten können Sie Enterprise Firmware Over the Air (E-FOTA) verwenden, um zu steuern, wann Firmware-Aktualisierungen von Samsung installiert werden. Durch die Kontrolle der Firmware-Versionen wird sichergestellt, dass die Geräte von Benutzern Firmware-Versionen verwenden, die ihre Apps unterstützen und die Richtlinien Ihres Unternehmens einhalten. Sie können ein Profil für Gerätedienstanforderungen verwenden, um Firmware-Regeln für die Samsung Knox-Geräte zu erstellen, die auf UEM aktiviert sind. Sie können programmieren, wann Firmware-Aktualisierungen installiert werden, und angeben, wann erzwungene Updates installiert werden müssen. Weitere Informationen zu E-FOTA finden Sie unter https://seap.samsung.com/sdk/enterprise-fota.

Bei Geräten, auf denen BlackBerry 10 OS-Version 10.3.1 oder höher ausgeführt wird und die mit Geschäftlich und persönlich – Reguliert oder Nur geschäftlicher Bereich aktiviert werden, können Sie mit einem Profil für Gerätedienstanforderungen begrenzen, welche Softwareversionen auf BlackBerry 10-Geräten installiert werden können. Darüber hinaus können Sie für bestimmte Gerätemodelle Ausnahmen zu den globalen Einstellungen hinzufügen. Dies ist beispielsweise hilfreich, wenn Sie eine Softwareversion testen möchten, bevor Sie sie für Ihr Unternehmen verfügbar machen.

Auf Geräten mit MDM-Steuerelemente-Aktivierungen können Sie nicht steuern, wann und wie Benutzer ihr Gerätebetriebssystem aktualisieren, aber Sie können bestimmte Gerätebetriebssystemversionen mithilfe von Konformitätsprofilen sperren. Um eine bestimmte Aktion auf allen Geräten zu erzwingen, wenn eine gesperrte Softwareversion auf einem Gerät installiert wird, müssen Sie ein Konformitätsprofil erstellen und dieses Benutzern, Benutzergruppen oder Gerätegruppen zuweisen. Das Kompatibilitätsprofil gibt an, welche Aktionen ausgeführt werden, wenn der Benutzer die gesperrte Softwareversion nicht vom Gerät löscht.

Sie können die auf iOS-Geräten installierten Softwareversionen nicht steuern, aber sie können die Installation eines verfügbaren Updates auf iOS-Geräten unter Aufsicht erzwingen. Weitere Informationen finden Sie unter Aktualisieren des Betriebssystems auf beaufsichtigten iOS-Geräten.

Erstellen eines Profils für Gerätedienstanforderungen für Android Enterprise-Geräte

Regeln für Betriebssystemaktualisierungen stehen nur für Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Geräte zur Verfügung. App-Aktualisierungsregeln gelten für alle Android Enterprise-Geräte. Weitere Informationen zum Festlegen von Regeln für Samsung Knox-Geräte, die E-FOTA verwenden, finden Sie unter Erstellen eines Profils für Gerätedienstanforderungen für Samsung Knox-Geräte.

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

2. Klicken Sie auf **Konformität > Gerätedienstanforderungen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Klicken Sie auf die Registerkarte **Android**.
6. Mithilfe folgender Schritte können Sie Regeln für Betriebssystemaktualisierungen auf Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Geräten festlegen:
   a) Klicken Sie in der Tabelle **Regeln für Betriebssystemaktualisierungen** auf +.
   b) Wählen Sie in der Dropdown-Liste **Gerätemodell** ein Gerätemodell aus.
   c) Wählen Sie in der Dropdown-Liste **Betriebssystemversion** die installierte Betriebssystemversion aus.
   d) Wählen Sie in der Dropdown-Liste **Aktualisierungsregel** eine der folgenden Optionen aus:
      - Wählen Sie **Standard**, wenn der Benutzer die Wahl haben soll, wann Updates installiert werden.
      - Wählen Sie **Automatisch aktualisieren**, wenn Aktualisierungen ohne Aufforderung an den Benutzer installiert werden sollen.
      - Wählen Sie **Automatisch aktualisieren zwischen**, um Aktualisierungen ohne Aufforderung an den Benutzer zwischen den von Ihnen angegebenen Zeiten zu installieren. Der Benutzer hat die Wahlmöglichkeit, Updates außerhalb dieses Zeitfensters zu installieren.
      - Wählen Sie **Verschieben um bis zu 30 Tage**, um die Installation von Updates für 30 Tage zu sperren. Nach 30 Tagen kann der Benutzer auswählen, wann ein Update installiert werden soll. Je nach Gerätehersteller und Mobilfunkanbieter werden Sicherheitsupdates möglicherweise nicht verschoben.
   e) Tippen Sie auf **Hinzufügen**, wenn Sie fertig sind.
   f) Wiederholen Sie Schritt 6 für jede Regel, die Sie hinzufügen möchten.

   Regeln für Samsung Knox-Geräte, die E-FOTA verwenden, haben Vorrang vor diesen Regeln.
7. Wenn Sie für Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Geräte Zeiträume angeben möchten, in denen keine Betriebssystemaktualisierungen durchgeführt werden sollen, führen Sie die folgenden Schritte aus:
   a) Klicken Sie in der Tabelle **Betriebssystemaktualisierung aussetzen** auf +.
   b) Wählen Sie in der Dropdown-Liste **Startmonat** den Monat aus, in dem der Aussetzungszeitraum beginnt.
   c) Wählen Sie in der Dropdown-Liste **Starttag** den Tag aus, an dem die Aussetzungszeitraum beginnt.
   d) Wählen Sie in der Dropdown-Liste **Dauer** die Länge des Zeitraums aus.

      Der Aussetzungszeitraum darf 90 Tage nicht überschreiten. Wenn Sie mehr als einen Aussetzungszeitraum angeben, müssen zwischen den Zeiträumen mindestens 60 Tage liegen.

      Diese Einstellungen gelten nicht für Samsung Knox-Geräte, die E-FOTA verwenden.
8. Wenn Sie einen Aktualisierungszeitraum für Apps festlegen möchten, die im Vordergrund ausgeführt werden, wählen Sie **Updatezeitraum für im Vordergrund laufende Apps aktivieren**, und nehmen Sie die folgenden Einstellungen vor:
   - **Startzeit (lokale Zeitzone des Geräts)**: Gibt die Uhrzeit an, zu der die Apps mit der Aktualisierung beginnen.
   - **Dauer**: Gibt die Anzahl der Stunden an, die Apps aktualisiert werden dürfen.
9. Wenn Sie festlegen möchten, wie Google Play die Änderungen auf Apps anwendet, die im Vordergrund ausgeführt werden, wählen Sie „Richtlinie für automatische App-Updates“ aus. Wählen Sie eine der folgenden Optionen aus:
   - **Benutzer kann zustimmen**: Der Benutzer wird aufgefordert, die Aktualisierung der Apps auf dem Gerät zuzulassen. Beachten Sie, dass dies die Standardeinstellung ist, wenn Sie nicht die Option „Richtlinie für automatische App-Updates“ auswählen.
   - **Immer**: Die Apps werden immer aktualisiert. Beachten Sie, dass Apps, die immer laufen, wie z. B. BlackBerry UEM Client, BlackBerry Work oder BlackBerry Connectivity, erst dann aktualisiert werden, wenn der Benutzer die Aktualisierung auf dem Gerät manuell durchführt, es sei denn, Sie wählen die Option „Updatezeitraum für im Vordergrund laufende Apps aktivieren“ aus.

- **Nur Wi-Fi**: Die Apps werden nur dann aktualisiert, wenn das Gerät mit einem Wi-Fi-Netzwerk verbunden ist. Beachten Sie, dass Apps, die immer laufen, wie z. B. BlackBerry UEM Client, BlackBerry Work oder BlackBerry Connectivity, erst dann aktualisiert werden, wenn der Benutzer die Aktualisierung auf dem Gerät manuell durchführt, es sei denn, Sie wählen die Option **Updatezeitraum für im Vordergrund laufende Apps aktivieren** aus.
- **Deaktivieren**: Die Apps werden nie aktualisiert.

  Hinweis:

  Dieses Profil wirkt sich auf die Einstellung „Apps automatisch aktualisieren“ in Google Play aus. Wenn Sie **Immer**, **Nur Wi-Fi** oder **Deaktivieren** wählen, kann der Benutzer keine andere Option auf dem Gerät auswählen. Wenn Sie beispielsweise im Profil **Deaktivieren** auswählen, kann der Benutzer die Aktualisierung einer App auf dem Gerät nicht aktivieren. Benutzer können Apps jedoch weiterhin manuell in Google Play aktualisieren.

10. Klicken Sie auf **Hinzufügen**.

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

Erstellen eines Profils für Gerätedienstanforderungen für Samsung Knox-Geräte

Bevor Sie beginnen: Überprüfen Sie, ob BlackBerry UEM eine E-FOTA-Lizenz hinzugefügt wurde. Um E-FOTA zu verwenden müssen Sie OTA-Aktualisierungen für Android-Geräte in der zugehörigen IT-Richtlinie in der BlackBerry UEM-Verwaltungskonsole zulassen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Konformität > Gerätedienstanforderungen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Klicken Sie auf die Registerkarte **Android**.
6. Klicken Sie in der Tabelle **Firmware-Regeln für Samsung-Geräte** auf +.
7. Geben Sie im Feld **Gerätemodell** das Gerätemodell ein, oder wählen Sie eines aus der Dropdown-Liste aus.
8. Wählen Sie in der Dropdown-Liste **Sprache** eine Sprache aus.
9. Geben Sie im Feld **Netzbetreibercode** den CSC-Code für den Mobilfunkanbieter für das Gerät ein.
10. Klicken Sie auf **Firmwareversion abrufen**.
11. Wiederholen Sie Schritt 5 bis 8 für jede Firmwareregel, die Sie hinzufügen möchten.
12. Tippen Sie auf **Hinzufügen**, wenn Sie fertig sind.
13. Klicken Sie in der Tabelle **Firmware-Regeln für Samsung-Geräte** neben der Firmware-Version, die Sie hinzugefügt haben, auf **Zeitplan**.
14. Gehen Sie im Dialogfeld **Erzwungene Aktualisierung planen** wie folgt vor:
    a) Wählen Sie in den Feldern **Erzwungene Aktualisierung planen zwischen** einen Datumsbereich aus, in dem das Update installiert werden muss. Der Datumsbereich muss zwischen 3 und 7 Tagen betragen. Der Standardwert ist 7 Tage.
    b) Geben Sie in den Dropdown-Listen **Erzwungene Aktualisierung planen in der Zeit von** an, wann die erzwungene Aktualisierung installiert werden muss und welche Zeitzone für den Benutzer gilt. Der Zeitraum muss zwischen 1 und 12 Stunden betragen.
15. Klicken Sie auf **Speichern**.

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

Hinzufügen einer E-FOTA-Lizenz

Mit Enterprise Firmware Over the Air (E-FOTA) können Sie steuern, wann Firmware-Aktualisierungen von Samsung auf Samsung Knox-Geräten installiert werden. Durch die Kontrolle der Firmware-Versionen wird sichergestellt, dass die Geräte von Benutzern Firmware-Versionen verwenden, die ihre Apps unterstützen und die Richtlinien Ihres Unternehmens einhalten.

Bevor Sie ein Gerätedienstanforderungsprofil zur Steuerung von Firmware-Versionen erstellen können, müssen Sie eine E-FOTA-Lizenz in UEM hinzufügen.

1. Klicken Sie in der Menüleiste auf **Lizenzierung** > **Lizenzierungsübersicht**.
2. Klicken Sie im Abschnitt **E-FOTA** auf **Lizenz hinzufügen**.
3. Geben Sie im Dialogfeld **E-FOTA-Lizenz hinzufügen** den Namen, die Client-ID, den geheimen Client-Schlüssel, die Kunden-ID und den Lizenzschlüssel ein.
4. Klicken Sie auf **Speichern**.

Erstellen eines Profils für Gerätedienstanforderungen für BlackBerry 10-Geräte

Bevor Sie beginnen: Erstellen oder bearbeiten Sie ein Kompatibilitätsprofil, das die Aktionen angibt, die ausgeführt werden, wenn eine gesperrte Softwareversion auf einem Gerät installiert wird.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie **Konformität > Gerätedienstanforderungen**
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Klicken Sie auf die Registerkarte **BlackBerry**.
6. Um eine Liste aller BlackBerry 10-Softwareversionen des Geräts und entsprechender Informationen zu Dienstanbieter, Gerätemodell, Hardware-ID, Softwareversion und Widerruf-Status anzuzeigen, klicken Sie auf **Anzeige einer Liste der Softwareversionen des Geräts**.
7. Aktivieren Sie das Kontrollkästchen **Update erforderlich machen**, um eine Aktualisierung des Geräts auf eine im Profil definierte Softwareversion durch den Benutzer zu erzwingen.
8. Geben Sie im Feld **Übergangsfrist** einen Wert in Stunden ein, der verstreichen kann, bevor die Geräte zwingend aktualisiert werden müssen. Wenn Benutzer ihre Geräte innerhalb der Übergangsfrist nicht aktualisieren, oder wenn Sie die Übergangsfrist auf 0 setzen, wird das Softwareupdate automatisch auf den Geräten installiert.
9. Wählen Sie in der Dropdown-Liste **Mindestens erforderliche Softwareversion** die Softwareversion aus, die mindestens auf einem BlackBerry 10-Gerät ausgeführt werden muss.
10. Wählen Sie in der Dropdown-Liste **Maximale Softwareversion** die maximale Softwareversion aus, die auf einem BlackBerry 10-Gerät ausgeführt werden muss.
11. Um die globalen Einstellungen für ein Gerätemodell zu überschreiben, führen Sie die folgenden Aufgaben aus:
    a) Klicken Sie in der Tabelle **Ausnahmen** auf +.
    b) Wählen Sie in der Dropdown-Liste **Verfügbarkeit** aus, ob Sie Softwareversionen zulassen oder nicht zulassen möchten. Wenn Sie einen nicht zulässigen Bereich angeben und keinen zulässigen Bereich für ein Gerätemodell angegeben haben, wird eine zweite Spalte eingeblendet, in der Sie einen zulässigen Bereich angeben müssen. Wenn kein zulässiger Bereich angegeben wird, gelten die globalen Einstellungen nicht mehr für das Gerätemodell, und alle Softwareversionen, abgesehen von Ausnahmen, werden automatisch zugelassen.
    c) Wählen Sie in der Dropdown-Liste **Gerätemodell** das Gerätemodell aus, für das Sie eine Ausnahme einrichten möchten.

d) Wählen Sie in der Dropdown-Liste **Mindestens** die mindestens erforderliche Softwareversion aus, die Sie zulassen oder nicht zulassen möchten.
e) Wählen Sie in der Dropdown-Liste **Maximum** die maximale Softwareversion aus, die Sie zulassen oder nicht zulassen möchten.
f) Wenn Sie eine Softwareversion nicht zugelassen haben, wählen Sie die mindestens erforderliche Softwareversion aus, die Sie zulassen möchten.
g) Wenn Sie eine Softwareversion nicht zugelassen haben, wählen Sie die maximale Softwareversion aus, die Sie zulassen möchten.

12. Klicken Sie auf **Speichern**.

13. Klicken Sie auf **Hinzufügen**.

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

Benutzer anzeigen, die eine widerrufene Softwareversion ausführen

Sie können eine Liste von Benutzern anzeigen, die eine widerrufene Softwareversion ausführen. Bei einer widerrufenen Softwareversion handelt es sich um eine Softwareversion, die von einem Dienstanbieter nicht mehr akzeptiert wird, aber möglicherweise noch auf dem Gerät eines Benutzers installiert ist.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie **Konformität > Gerätedienstanforderungen**.
3. Klicken Sie auf den Namen des Profils, das Sie anzeigen möchten.
4. Klicken Sie auf die Registerkarte **{0} Benutzer mit einer gesperrten Softwareversion**, um die Liste von Benutzern anzuzeigen, die eine widerrufene Softwareversion ausführen.

Verwalten von Betriebssystem-Updates auf Geräten mit MDM-Steuerelemente-Aktivierungen

Sie können nicht steuern, wann Softwareversionen auf MDM-Steuerelemente-Geräten mit -Aktivierungen installiert werden. Mithilfe von Konformitätsprofilen können Sie jedoch Geräte steuern, die Benutzer auf eine Betriebssystemversion aktualisiert haben, die Ihr Unternehmen nicht zulässt. Beispielsweise unterstützen Android-Geräte ab Version 10 keine MDM-Steuerelemente-Aktivierungen. Wenn Benutzer mit Android 9.x-Geräten auf Android 10 aktualisieren, funktionieren einige Geräteverwaltungsfunktionen nicht mehr, sodass das Gerät in einem infizierten Zustand bleibt. Sie können Gerätegruppen und Konformitätsprofile verwenden, um Android Geräte mit dem Aktivierungstyp MDM-Steuerelemente zu erkennen und Konformitätsregeln festzulegen, um geeignete Maßnahmen zu ergreifen, z. B. Benutzer benachrichtigen oder das Gerät als nicht vertrauenswürdig oder nicht steuerbar kennzeichnen.

Führen Sie die folgenden Schritte aus, um Betriebssystem-Updates auf Geräten mit MDM-Steuerelemente-Aktivierungen zu verwalten.

Schritt	Aktion
1	Erstellen Sie eine Gerätegruppe, die Geräte enthält, die den folgenden Parametern entsprechen: • MDM-Steuerelemente-Aktivierungstyp • Geräte-Betriebssystemversion, die Sie einschränken möchten Wenn ein Benutzer ein Gerät auf das angegebene Betriebssystem aktualisiert, wird es automatisch Teil der Gerätegruppe.
2	Erstellen Sie ein Konformitätsprofil, und geben Sie die Version des Gerätebetriebssystems als gesperrte Betriebssystemversion an.
3	Geben Sie im Konformitätsprofil die für Ihr Unternehmen geeignete Erzwingungsaktion an. Sie können beispielsweise den Benutzer benachrichtigen, dass sein Aktivierungstyp nicht vom Gerätebetriebssystem unterstützt wird, und empfehlen, das Gerät mit einem anderen Aktivierungstyp neu zu aktivieren oder das Gerät zu deaktivieren.
4	Weisen Sie das Konformitätsprofil der Gerätegruppe zu.
5	Erstellen Sie optional eine Ereignisbenachrichtigung, um Administratoren zu informieren, wenn ein Gerät in Bezug auf das Konformitätsprofil nicht richtlinienkonform ist.

Anzeigen verfügbarer Updates für iOS-Geräte

Sie können sehen, ob ein Softwareupdate für die iOS-Geräte der Benutzer verfügbar ist und sie dazu veranlassen, ein Update auf die neueste Version durchzuführen.

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. Ob ein Update verfügbar ist, wird im Abschnitt für das aktivierte Gerät angezeigt.

Aktualisieren des Betriebssystems auf beaufsichtigten iOS-Geräten

Sie können die Installation eines verfügbaren Betriebssystem-Updates auf iOS-Geräten erzwingen. Informationen zur Aktualisierung des Betriebssystems auf mehreren Geräten finden Sie unter Senden eines Stapelbefehls.

Sie können auch die zeitliche Planung von iOS-Softwareupdates mithilfe der IT-Richtlinienregeln „Verzögerung von Softwareupdates“ und „Verzögerungszeit für Softwareupdates“ steuern. Weitere Informationen finden Sie in der Richtlinien-Referenztabelle.

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. Wenn ein Softwareupdate verfügbar ist, klicken Sie im linken Fensterbereiche auf **Jetzt aktualisieren**.
6. Wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus:
   - **Herunterladen und installieren**: Das Update wird automatisch heruntergeladen und auf dem Gerät installiert.
   - **Nur herunterladen**: Das Update wird automatisch auf das Gerät heruntergeladen, und der Benutzer wird aufgefordert, es zu installieren.
   - **Heruntergeladene Aktualisierungen installieren**: Wenn das Update bereits auf ein Gerät heruntergeladen wurde, wird es automatisch installiert.
7. Wählen Sie in der Liste **OS-Version** die Betriebssystemversion aus, auf die Sie das Gerät aktualisieren möchten.
8. Klicken Sie auf **Aktualisieren**.

Konfigurieren der Kommunikation zwischen Geräten und BlackBerry UEM

Das Enterprise Management Agent-Profil stellt sicher, dass Geräte regelmäßig BlackBerry UEM für App- oder Konfigurations-Updates kontaktieren. Wenn es ein Update für ein Gerät gibt, fordert BlackBerry UEM das Gerät dazu auf, BlackBerry UEM zu kontaktieren, um die Updates abzurufen. Wenn das Gerät aus irgendeinem Grund die Aufforderung nicht erhält, wird das Enterprise Management Agent-Profil verwendet, um dafür zu sorgen, dass das Gerät BlackBerry UEM in von Ihnen festgelegten Intervallen kontaktiert.

In lokalen Umgebungen können Sie außerdem das Enterprise Management Agent-Profil verwenden, um BlackBerry UEM zu erlauben, eine Liste von persönlichen Apps auf den Geräten von Benutzern zu erfassen. Zum Ausschalten der Sammlung von persönlichen Apps müssen Sie die Einstellung „Sammlung von persönlichen Apps zulassen“ deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der Sammlung persönlicher Apps.

Bei BlackBerry 10-Geräten können Sie über das Enterprise Management Agent-Profil einschränken, welche Cipher Suites der SSL-Bibliothek von dem Gerät unterstützt werden. Die Beschränkung der unterstützten Cipher Suites hat keine Auswirkungen auf die Kommunikation des Geräts mit BlackBerry UEM, könnte aber Auswirkungen auf die Kommunikation mit anderen Servern in Ihrem Unternehmen, je nach Anforderungen dieser Server haben.

Sie können den Benutzern, Benutzergruppen und Gerätegruppen ein Enterprise Management Agent-Profil zuweisen.

Erstellen eines Enterprise Management Agent-Profils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinie > Enterprise Management Agent**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Legen Sie die Werte für jeden Gerätetyp wie von Ihrem Unternehmen vorgeschrieben fest.
6. Klicken Sie auf **Hinzufügen**.

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

iOS: Enterprise Management Agent-Profileinstellungen

Einstellung	Beschreibung
Enterprise Management Agent-Abfragerate	Geben Sie in Sekunden an, wie häufig das Gerät Enterprise Management Agent-Serverbefehle abruft. Das Gerät fragt nur ab, wenn der UEM Client auf dem Gerät geöffnet ist. Mögliche Werte: • 900 bis 86400 Der Standardwert ist 3600.

Einstellung	Beschreibung
Sammlung von persönlichen Apps zulassen	Diese Einstellung legt fest, ob BlackBerry UEM eine Liste mit persönlichen Apps enthält, die auf den Geräten der Benutzer installiert sind. Diese Einstellung wird nicht auf Geräten mit Benutzerdatenschutzaktivierungen unterstützt.

Android: Enterprise Management Agent-Profileinstellungen

Einstellung	Beschreibung
App-Änderungen	Geben Sie in Sekunden an, wie häufig das Gerät installierte Apps auf Änderungen prüft. Mögliche Werte: • 3600 bis 86400 Sekunden Der Standardwert ist 3600.
Akku-Grenzwert	Legen Sie den Grenzwert für den Akku-Ladestand in Prozent (von 5 bis 100) fest, der vor dem Zurücksenden von Informationen vom Gerät an BlackBerry UEM erforderlich ist. Mögliche Werte: • 5 bis 100 Prozent Der Standardwert ist 20.
Grenzwert für freien RAM-Speicherplatz	Legen Sie den Grenzwert für den freien Speicherplatz in Megabytes fest, der vor dem Zurücksenden von Informationen vom Gerät an BlackBerry UEM erforderlich ist. Standardmäßig sendet das Gerät diese Informationen nicht zurück an BlackBerry UEM.
Grenzwert für internen Speicher	Legen Sie den Grenzwert für den internen freien Speicherplatz in Megabytes fest, der vor dem Zurücksenden von Informationen vom Gerät an BlackBerry UEM erforderlich ist. Der Standardwert ist 250.
Grenzwert für Speicherkarte	Legen Sie den Grenzwert für den externen freien Speicherplatz in Megabytes fest, der vor dem Zurücksenden von Informationen vom Gerät an BlackBerry UEM erforderlich ist. Der Standardwert ist 500.
Enterprise Management Agent-Abfragerate	Geben Sie in Sekunden an, wie häufig das Gerät Enterprise Management Agent-Serverbefehle abruft. Mögliche Werte: • Minimum: 900 Der Standardwert ist 900.

Einstellung	Beschreibung
Sammlung von persönlichen Apps zulassen	Diese Einstellung legt fest, ob BlackBerry UEM eine Liste mit persönlichen Apps enthält, die auf den Geräten der Benutzer installiert sind. Diese Einstellung wird nicht auf Geräten mit Benutzerdatenschutzaktivierungen unterstützt.

Windows: Enterprise Management Agent-Profileinstellungen

Einstellung	Beschreibung
Abfrageintervall für Konfigurationsupdates	Legen Sie fest, wie häufig das Gerät Konfigurationsupdates abruft (in Minuten), wenn Push-Benachrichtigungen nicht verfügbar sind.
Abfrageintervall für die erste Auswahl von Wiederholungsversuchen	Geben Sie die Wartezeit in Minuten zwischen den Versuchen in der ersten Reihe von Wiederholungen an, wenn die Abfrage nach Gerätekonfigurations-Updates fehlschlägt.
Anzahl der ersten Wiederholungsversuche	Geben Sie die Anzahl der Versuche in der ersten Reihe von Wiederholungen an.
Abfrageintervall für die zweite Auswahl von Wiederholungsversuchen	Geben Sie die Wartezeit in Minuten zwischen den Versuchen in der zweiten Reihe von Wiederholungen an, wenn die Abfrage nach Gerätekonfigurations-Updates fehlschlägt.
Anzahl der zweiten Wiederholungsversuche	Geben Sie die Anzahl der Versuche in der zweiten Reihe von Wiederholungen an.
Abfrageintervall für die verbleibenden geplanten Wiederholungsversuche	Geben Sie die Wartezeit in Minuten zwischen den Folgeversuchen nach der zweiten Reihe von Wiederholungen an, wenn die Abfrage für die Gerätekonfigurations-Updates fehlschlägt.
Anzahl der verbleibenden Wiederholungsversuche	Geben Sie Anzahl der Folgeversuche nach der zweiten Reihe von Wiederholungen an, wenn die Abfrage nach Gerätekonfigurations-Updates fehlschlägt. Bei Einstellung auf „0“ fragt das Gerät weiterhin ab, bis eine Verbindung erfolgreich hergestellt oder das Gerät deaktiviert wird.
Bei Benutzeranmeldung abrufen	Legen Sie fest, ob das Gerät bei Anmeldung eines Benutzers eine Verwaltungssitzung startet.
Alle Benutzer bei erstmaliger Anmeldung abrufen	Legen Sie fest, ob das Gerät eine Verwaltungssitzung bei erstmaliger Benutzeranmeldung für alle Benutzer startet.
Sammlung von persönlichen Apps zulassen	Diese Einstellung legt fest, ob BlackBerry UEM eine Liste mit persönlichen Apps enthält, die auf den Geräten der Benutzer installiert sind.

BlackBerry 10: Enterprise Management Agent-Profileinstellungen

Einstellung	Beschreibung
Abfrageintervall des Enterprise Management Web Service	Geben Sie in Sekunden an, wie häufig Enterprise Management Web Service Konfigurations-Updates auf dem Gerät abruft. Mögliche Werte: • 3600 bis 86400 Der Standardwert ist 3600.
Schnelles Abfrageintervall	Geben Sie an (in Sekunden), wie häufig das Gerät Konfigurationsupdates abruft, wenn Push-Benachrichtigungen für schnelle Abfragen nicht verfügbar sind (BDPS ist nicht registriert). • Minimum: 900 Der Standardwert ist 900.
Langsames Abfrageintervall	Geben Sie an (in Sekunden), wie häufig das Gerät Konfigurationsupdates abruft, wenn Push-Benachrichtigungen für langsame Abfragen verfügbar sind (BDPS ist nicht registriert). • Minimum: 900 Der Standardwert ist 900.
Sammlung von persönlichen Apps zulassen	Diese Einstellung legt fest, ob BlackBerry UEM eine Liste mit persönlichen Apps enthält, die auf den Geräten der Benutzer installiert sind. Diese Einstellung wird nicht auf Geräten mit Aktivierungsart „Geschäftlich und persönlich – Unternehmen“ unterstützt.

Einstellung	Beschreibung
Konfigurationsdatei (.json)	Mit dieser Einstellung können Sie eine Konfigurationsdatei festlegen, die die von dem Gerät unterstützten Cipher Suites aus der SSL-Bibliothek beschränkt. Geben Sie diese Konfigurationsdatei nur an, wenn die Unterstützung für eine Cipher Suite entfernt werden soll, die ein Sicherheitsrisiko darstellt, und die Ressourcen Ihrer Organisation diese Cipher Suite für die Kommunikation nicht benötigen. Die Konfigurationsdatei hat keine Auswirkungen auf die Kommunikation des Geräts mit BlackBerry UEM, könnte aber Auswirkungen auf die Kommunikation mit anderen Servern in Ihrer Organisation, je nach Anforderungen dieser Server, haben. Die Konfigurationsdatei muss das JSON-Format aufweisen. **Beispiel:** `{"tls": {"tls_protocols": ["TLSv1"], "tls_ciphersuites": [49200, 49196, 49192, 49188, 49172, 49162, 163, 159, 107, 106, 57, 56, 136, 135, 49202, 49198, 49194, 49190, 49167, 49157, 157, 61, 53, 132, 141, 49199, 49195, 49191, 49187, 49171, 49161, 162, 158, 103, 64, 51, 50, 154, 153, 69, 68, 49201, 49197, 49193, 49189, 49166, 49156, 156, 60, 47, 150, 65, 140, 49169, 49159, 49164, 49154, 5, 4, 138, 49170, 49160, 22, 19, 49165, 49155, 10, 139, 21, 18, 9, 20, 17, 8, 6, 3], "tls_curves": ["secp256r1", "secp521r1", "brainpoolP512r1", "brainpoolP384r1", "secp384r1", "brainpoolP256r1", "secp256k1", "sect571r1", "sect571k1", "sect409k1", "sect409r1", "sect283k1", "sect283r1", "secp224k1", "secp224r1", "secp192k1", "secp192r1", "secp160k1", "secp160r1", "secp160r2", "sect239k1", "sect233k1", "sect233r1", "sect193r1", "sect193r2", "sect163k1", "sect163r1", "sect163r2"], "tls_sigalgs": ["ECDSA+SHA512", "DSA+SHA512", "RSA+SHA512", "ECDSA +SHA384", "DSA+SHA384", "RSA+SHA384", "ECDSA+SHA256", "DSA +SHA256", "RSA+SHA256", "ECDSA+SHA224", "DSA+SHA224", "RSA+SHA224", "ECDSA+SHA1", "DSA+SHA1", "RSA+SHA1"], "tls_dh_min_key_bits":768, "tls_suiteb_mode": "SUITEB_OFF"}, "vpn": {"vpn_encr": ["aes128", "aes256", "aes128_icv16_gcm", "aes256_icv16_gcm", "3des", "aes192"], "vpn_dh": ["dh2", "dh5", "dh7", "dh8", "dh9", "dh10", "dh11", "dh12", "dh13", "dh14", "dh15", "dh16", "dh17", "dh18", "dh19", "dh20", "dh21", "dh22", "dh23", "dh24", "dh25", "dh26"], "vpn_integ": ["sha1", "sha384", "sha512", "aes", "sha256"], "vpn_prf": ["sha1", "sha384", "sha512", "aes", "hmac", "sha256"]}}`

Anzeigen von Organisationsinformationen auf Geräten

Sie können BlackBerry UEM so konfigurieren, dass auf den Geräten Organisationsinformationen und benutzerdefinierte Organisationshinweise angezeigt werden.

Für BlackBerry 10-, iOS-, macOS-, Android- und Windows 10-Geräte können Sie benutzerdefinierte Organisationshinweise erstellen und einstellen, sodass sie während der Aktivierung angezeigt werden. Beispielsweise kann ein Hinweis die Bedingungen enthalten, die ein Benutzer befolgen muss, um die Sicherheitsanforderungen in Ihrem Unternehmen zu erfüllen. Der Benutzer muss den Hinweis bestätigen, um mit dem Aktivierungsprozess fortfahren zu können. Sie können mehrere Hinweise erstellen und so verschiedene Anforderungen abdecken. Darüber hinaus können Sie auch separate Versionen der einzelnen Hinweise erstellen, um verschiedene Sprachen zu unterstützen.

Sie können Geräteprofile zum Anzeigen von Informationen zu Ihrem Unternehmen auf Geräten erstellen. Im Falle von iOS- und Android-Geräten werden die Organisationsinformationen im BlackBerry UEM Client auf dem Gerät angezeigt. Im Falle von Windows 10 werden die Telefonnummer und die E-Mail-Adresse in den Support-Informationen auf dem Gerät angezeigt. Im Falle von BlackBerry 10- und Samsung Knox-Geräten können Sie das Geräteprofil verwenden, um den benutzerdefinierten Organisationshinweis anzuzeigen, wenn der Benutzer das Gerät startet.

Bei BlackBerry 10-, Samsung Knox- und überwachten iOS-Geräten können Sie das Geräteprofil auch zum Hinzufügen eines benutzerdefinierten Hintergrundbilds verwenden, um Informationen für Ihre Benutzer anzuzeigen. Sie können beispielsweise ein Bild erstellen, das Kontaktinformationen für den Support, Informationen zu einer internen Website oder das Logo Ihres Unternehmens enthält. Auf BlackBerry 10- und Samsung Knox-Geräten wird der Hintergrund im geschäftlichen Bereich angezeigt.

Wo werden Unternehmensinformationen angezeigt?	Wie wird der Organisationshinweis konfiguriert?
Anzeige eines Organisationshinweises bei der Aktivierung auf BlackBerry 10-, iOS-, macOS-, Android- und Windows 10-Geräten	Erstellen Sie einen Organisationshinweis, und weisen Sie ihn einem Aktivierungsprofil zu.
Anzeige eines Organisationshinweises beim Neustart auf Samsung Knox-Geräten	Erstellen Sie einen Organisationshinweis, und weisen Sie ihn auf der Registerkarte Android des Geräteprofils zu. Um den Hinweis zu ändern, der beim Geräteneustart angezeigt wird, müssen Sie das Geräteprofil aktualisieren.
Anzeige eines Organisationshinweises beim Neustart auf BlackBerry 10-Geräten	Erstellen Sie einen Organisationshinweis, und weisen Sie ihn auf der Registerkarte BlackBerry eines Geräteprofils zu. Vergewissern Sie sich, dass die IT-Richtlinie „Organisationshinweis nach Geräteneustart anzeigen“ ausgewählt wurde. Um den Hinweis zu ändern, der beim Geräteneustart angezeigt wird, müssen Sie das Geräteprofil aktualisieren. **Hinweis:** Die IT-Richtlinie gilt nur für die Aktivierungsarten „Nur Geschäftlich“ und „Geschäftlich und persönlich – Reguliert“ auf Geräten, auf denen die BlackBerry 10 OS-Version 10.3.1 oder höher läuft.

Wo werden Unternehmensinformationen angezeigt?	Wie wird der Organisationshinweis konfiguriert?
In den Unternehmensinformationen im BlackBerry UEM Client auf iOS- oder Android-Geräten oder in den Supportinformationen auf Windows 10-Geräten.	Geben Sie die Informationen, die Sie anzeigen möchten, in die entsprechende Registerkarte des Geräteprofils ein.
In einem Hintergrundbild auf BlackBerry 10-, Samsung Knox- oder überwachten iOS-Geräten.	Wählen Sie eine Bilddatei auf der entsprechenden Registerkarte des Geräteprofils aus.

Erstellen von Organisationshinweisen

Sie können benutzerdefinierte Organisationshinweise verwenden, die bei der Aktivierung von BlackBerry 10-, iOS-, macOS-, Android- und Windows 10-Geräten angezeigt werden.

BlackBerry 10- und Samsung Knox-Geräte können den Organisationshinweis auch anzeigen, wenn ein Benutzer das Gerät neu startet.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Erweitern Sie im linken Fensterbereich die Option **Allgemeine Einstellungen**.
3. Klicken Sie auf **Organisationshinweise**.
4. Klicken Sie am rechten Bildschirmrand auf +.
5. Geben Sie im Feld **Name** einen Namen für den Organisationshinweis ein.
6. Optional können Sie auch den Text aus einem bereits vorhandenen Organisationshinweis übernehmen, indem Sie ihn in der Dropdown-Liste **Kopierter Text aus Organisationshinweis** auswählen.
7. Wählen Sie in der Dropdown-Liste **Gerätesprache** die Sprache aus, die für den Organisationshinweis als Standardsprache verwendet werden soll.
8. Geben Sie im Feld **Organisationshinweis** den Text des Organisationshinweises ein.
9. Optional können Sie mehrmals auf **Hinzufügen einer weiteren Sprache** klicken, um den Organisationshinweis in mehreren Sprachen zu posten.
10. Wenn Sie den Organisationshinweis in mehr als einer Sprache veröffentlichen, wählen Sie die Option **Standardsprache** unter einer der Nachrichten, um die Standardsprache festzulegen.
11. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Wenn der Unternehmenshinweis während der Aktivierung angezeigt werden soll, weisen Sie den Unternehmenshinweis einem Aktivierungsprofil zu.
- Um den Organisationshinweis während des Neustarts eines Samsung Knox Geräts anzuzeigen, weisen Sie den Organisationshinweis einem Geräteprofil zu.
- Um einen Unternehmenshinweis beim Neustart eines BlackBerry 10-Geräts anzuzeigen, weisen Sie den Unternehmenshinweis einem Geräteprofil zu, und wählen Sie die IT-Richtlinienregel „Unternehmenshinweis nach Geräteneustart anzeigen“ aus.

Erstellen eines Geräteprofils

Bevor Sie beginnen: Erstellen Sie Unternehmenshinweise für BlackBerry 10- und Samsung Knox-Geräte.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Benutzerdefiniert > Gerät**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Geräteprofil muss über einen eindeutigen Namen verfügen.
5. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Zuweisen eines Organisationshinweises zur Anzeige auf BlackBerry 10- oder Samsung Knox-Geräten während des Geräteneustarts	a. Klicken Sie auf **BlackBerry** oder **Android**. b. Wählen Sie in der Dropdown-Liste **Organisationshinweis zuweisen** den Organisationshinweis aus, der auf Geräten angezeigt werden soll.
Definieren Sie für iOS- oder Android-Geräte die Unternehmensinformationen, die in der BlackBerry UEM Client-App angezeigt werden sollen. Definieren Sie für Windows 10 die Telefonnummer und E-Mail-Adresse, die in den Support-Informationen auf Geräten angezeigt werden sollen.	a. Klicken Sie auf **iOS**, **Android** oder **Windows**. b. Geben Sie den Namen, die Adresse, Telefonnummer und E-Mail-Adresse Ihrer Organisation ein.

6. Führen Sie ggf. die folgenden Aufgaben aus:

Aufgabe	Schritte
Hinzufügen eines Hintergrundbilds zum geschäftlichen Bereich auf BlackBerry 10- oder Samsung Knox-Geräten	a. Klicken Sie auf **BlackBerry** oder **Android**. b. Klicken Sie im Bereich **Hintergrundbild für den geschäftlichen Bereich** auf **Durchsuchen**. c. Wählen Sie das gewünschte Bild aus. d. Klicken Sie auf **Öffnen**.
Hinzufügen eines Hintergrundbilds bei überwachten iOS-Geräten	a. Klicken Sie auf **iOS**. b. Wählen Sie im Abschnitt **Hintergrundbild des Gerätes** aus, ob das Hintergrundbild auf dem **Startbildschirm**, auf dem **Sperrbildschirm**, oder auf **beiden** angezeigt werden soll. c. Klicken Sie auf **Durchsuchen**, und wählen Sie das gewünschte Bild aus. d. Klicken Sie auf **Öffnen**. e. Im Feld **Hintergrundbild festlegen für** wählen Sie aus, wo das Hintergrundbild angezeigt werden soll.

7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Um einen Unternehmenshinweis beim Neustart eines BlackBerry 10-Geräts anzuzeigen, wählen Sie die IT-Richtlinienregel „Unternehmenshinweis nach Geräteneustart anzeigen“ aus.

- Legen Sie ggf. eine Rangfolge für die Profile fest.

Verwenden von Standortdiensten auf Geräten

Mithilfe eines Profils für die Standortbestimmung können Sie den Standort von Geräten anfordern und deren ungefähre Position auf einer Karte anzeigen. Sie können Benutzern auch ermöglichen, den Standort ihrer Geräte mithilfe von BlackBerry UEM Self-Service zu bestimmen. Wenn Sie den Standortverlauf für iOS- und Android-Geräte aktivieren, müssen die Geräte regelmäßig Standortinformationen melden. Administratoren können den Standortverlauf anzeigen.

In Profilen für die Standortbestimmung werden die Standortdienste auf iOS-, Android- und Windows 10 Mobile-Geräten verwendet. Je nach Gerät und verfügbaren Diensten können Standortdienste Informationen von GPS, Mobilfunknetzen und Wi-Fi-Netzwerken verwenden, um die Position des Geräts zu bestimmen.

Konfigurieren der Einstellungen für die Standortbestimmung

Sie können die Einstellungen für Profile für die Standortbestimmung konfigurieren. Hierzu zählt die angezeigte Geschwindigkeitseinheit für ein Gerät, wenn dessen Standort auf einer Karte angezeigt wird. Wenn Sie den Standortverlauf für iOS- und Android-Geräte aktivieren, wird der Standortverlauf von BlackBerry UEM standardmäßig einen Monat lang gespeichert.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Standortbestimmung**.
2. Geben Sie in einer lokalen Umgebung im Feld **Alter des Standortverlaufs** die Anzahl der Tage, Wochen oder Monate an, für die BlackBerry UEM den Standortverlauf für Geräte speichert.
3. Klicken Sie in der Dropdown-Liste **Angezeigte Geschwindigkeitseinheit** auf **km/h** oder **mph**.
4. Klicken Sie auf **Speichern**.

Erstellen eines Profils für die Standortbestimmung

Sie können Benutzerkonten, Benutzergruppen und Gerätegruppen ein Profil für die Standortbestimmung zuweisen. Benutzer müssen das Profil akzeptieren, bevor die Verwaltungskonsole oder BlackBerry UEM Self-Service die Standorte von iOS- und Android-Geräten auf einer Karte anzeigen kann. Windows 10 Mobile-Geräte akzeptieren das Profil automatisch.

Bevor Sie beginnen: Konfigurieren der Einstellungen für die Standortbestimmung

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Schutz > Standortdienst**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil für die Standortbestimmung ein.
5. Deaktivieren Sie optional das Kontrollkästchen für alle Gerätetypen, für die Sie das Profil nicht konfigurieren möchten.
6. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Aktivieren des Standortverlaufs für iOS-Geräte	**a.** Überprüfen Sie auf der Registerkarte **iOS**, ob das Kontrollkästchen **Gerätestandortverlauf protokollieren** aktiviert ist. **Hinweis:** BlackBerry UEM erfasst die Standortdaten eines Geräts stündlich und wenn sich der Standort erheblich verändert (zum Beispiel 500 Meter oder mehr).
Aktivieren des Standortverlaufs für Android-Geräte	**a.** Überprüfen Sie auf der Registerkarte **Android**, ob das Kontrollkästchen **Gerätestandortverlauf protokollieren** aktiviert ist. **b.** Geben Sie im Feld **Entfernung für Gerätestandortprüfung** die minimale Entfernung an, die ein Gerät zurücklegen muss, bevor der Standort des Geräts aktualisiert wird. **c.** Geben Sie im Feld **Häufigkeit der Standortaktualisierung** an, wie oft der Gerätestandort aktualisiert wird. **Hinweis:** Die Bedingungen für die Entfernung und die Häufigkeit müssen erfüllt sein, bevor der Gerätestandort aktualisiert wird.

7. Klicken Sie auf **Hinzufügen**.

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

Standort eines Geräts bestimmen

Sie können iOS-, Android und Windows 10 Mobile-Geräte orten (z. B, wenn ein Gerät verloren geht oder gestohlen wird). Benutzer müssen das Profil für die Standortbestimmung akzeptieren, bevor die Verwaltungskonsole die Standorte von iOS- und Android-Geräten auf einer Karte anzeigen kann. Windows 10 Mobile-Geräte akzeptieren das Profil automatisch. Der Standortverlauf ist für iOS- und Android-Geräte verfügbar, wenn Sie diesen im Profil aktiviert haben.

Bevor Sie beginnen: Erstellen Sie ein Profil für die Standortbestimmung, und weisen Sie es zu.

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Deaktivieren Sie das Kontrollkästchen für jedes Gerät, dessen Standort Sie bestimmen möchten.
3. Klicken Sie auf .
4. Ermitteln Sie die Geräte auf der Karte mithilfe der folgenden Symbole. Wenn ein iOS- oder Android-Gerät nicht mit den neuesten Informationen zum Standort antwortet und der Standortverlauf im Profil aktiviert ist, zeigt die Karte die letzte bekannte Position des Geräts an.

   - Aktueller Standort:
   - Letzter bekannter Standort:

   Sie können auf ein Symbol klicken oder den Mauszeiger über ein Symbol bewegen, um Standortinformationen anzuzeigen, wie beispielsweise Längen- und Breitengrad und wann die Position gemeldet wurde (zum Beispiel vor 1 Minute oder vor 2 Stunden).
5. Um den Standortverlauf für ein iOS- oder Android-Gerät anzuzeigen, führen Sie die folgenden Aktionen aus:
   a) Klicken Sie auf **Standortverlauf anzeigen**.
   b) Wählen Sie einen Datums- und Zeitbereich aus.
   c) Klicken Sie auf **Senden**.

Verwenden des Verloren-Modus für iOS-Geräte unter Aufsicht

Sie können den Verloren-Modus für iOS-Geräte unter Aufsicht aktivieren und verwalten. Wenn ein Gerät verloren geht, ermöglicht Ihnen der Verloren-Modus Folgendes:

- Das Gerät sperren und eine Nachricht festlegen, die angezeigt werden soll (Sie können z. B. Kontaktinformationen anzeigen lassen, für den Fall, dass das Gerät gefunden wird)
- Den aktuellen Standort des Geräts anzeigen, ohne ein Standortdienstprofil zu verwenden
- Alle Geräte, die sich im Verloren-Modus befinden, über die Verwaltungskonsole nachverfolgen

Verloren-Modus aktivieren

Der Verloren-Modus wird auf überwachten iOS-Geräten unterstützt.

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Klicken Sie auf ein Gerät, für das Sie den Verloren-Modus aktivieren möchten.
3. Klicken Sie in der Geräteregisterkarte auf **Verloren-Modus aktivieren**.
4. Geben Sie in den Feldern **Kontakttelefonnummer** und **Nachricht** die entsprechenden Informationen ein.
5. Wählen Sie optional **Text „Zum Entsperren streichen“ ersetzen**, und geben Sie den Text ein, den Sie anzeigen möchten.
6. Klicken Sie auf **Aktivieren**.

Bestimmen des Standorts eines Geräts im Verloren-Modus

Bevor Sie beginnen: Verloren-Modus aktivieren

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Klicken Sie auf ein Gerät, bei dem der Verloren-Modus aktiviert ist.
3. Klicken Sie in der Geräte-Registerkarte auf **Gerätestandort abrufen**.

Deaktivieren des Verloren-Modus

Bevor Sie beginnen: Verloren-Modus aktivieren

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Klicken Sie auf ein Gerät, bei dem der Verloren-Modus aktiviert ist.
3. Klicken Sie in der Geräteregisterkarte auf **Verloren-Modus deaktivieren**.

Verwenden von Aktivierungssperren auf iOS-Geräten

Die Aktivierungssperre auf iOS-Geräten ermöglicht den Schutz von verlorenen oder gestohlenen Geräten. Wenn diese Funktion aktiviert ist, muss der Benutzer die Apple-ID und das Kennwort bestätigen, um „Mein iPhone suchen“ zu deaktivieren, das Gerät zu löschen oder das Gerät zu reaktivieren und zu verwenden.

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.

Wenn ein Gerät für die Nutzung von BlackBerry UEM aktiviert wurde, ist die Aktivierungssperre standardmäßig deaktiviert. Sie können sie für jedes Gerät einzeln aktivieren, oder Sie können sie mithilfe der IT-Unternehmensrichtlinien durchsetzen. Wenn Sie die Aktivierungssperre aktivieren, speichert BlackBerry UEM einen Umgehungscode zum Löschen der Sperre, mit dem das Gerät ohne Eingabe von Apple-ID und Kennwort des Benutzers gelöscht und erneut aktiviert werden kann.

Aktivierungssperre aktivieren

Führen Sie die folgenden Schritte durch, um die Aktivierungssperre für jedes Gerät einzeln zu aktivieren. Wenn die Aktivierungssperre mithilfe der IT-Richtlinienregel erzwungen wird, ist sie bereits aktiviert.

Hinweis: Wenn Sie die Aktivierungssperre aktivieren, tritt zwischen BlackBerry UEM und Apple möglicherweise eine kurze Verzögerung auf.

Bevor Sie beginnen:

- 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.

1. Klicken Sie in der Menüleiste auf **Benutzer**.
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. Klicken Sie im Fenster **Gerät verwalten** auf **Aktivierungssperre aktivieren**.

Wenn Sie fertig sind: Informationen zum Anzeigen des Umgehungscodes für Geräte finden Sie unter Umgehungscode für Aktivierungssperre anzeigen

Aktivierungssperre deaktivieren

Führen Sie die folgenden Schritte durch, um die Aktivierungssperre für jedes Gerät einzeln zu deaktivieren. Wenn die Aktivierungssperre mithilfe einer IT-Richtlinienregel erzwungen wird, können Sie sie nicht deaktivieren.

Hinweis: Wenn Sie die Aktivierungssperre aktivieren, tritt zwischen BlackBerry UEM und Apple möglicherweise eine kurze Verzögerung auf.

1. Klicken Sie in der Menüleiste auf **Benutzer**.
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** die Option **Aktivierungssperre deaktivieren** aus.

Umgehungscode für Aktivierungssperre anzeigen

Sie können den Umgehungscode für die Aktivierungssperre sowie das Erstellungsdatum des Umgehungscodes anzeigen.

1. Klicken Sie in der Menüleiste auf **Benutzer > Apple-Aktivierungssperre**.
2. Suchen Sie ein Gerät.
3. Klicken Sie in den Suchergebnissen auf das Gerät.
4. Scrollen Sie ggf. auf dem Hauptbildschirm nach rechts, um den Umgehungscode anzuzeigen.

Verwalten von iOS-Funktionen mit benutzerdefinierten Payload-Profilen

Mit benutzerdefinierten Payload-Profilen können Sie Funktionen auf iOS-Geräten steuern, die nicht durch bestehende BlackBerry UEM-Richtlinien oder -Profile gesteuert werden.

Hinweis: Wenn eine Funktion durch eine vorhandene BlackBerry UEM-Richtlinie oder ein Profil geregelt ist, funktioniert eventuell ein benutzerdefiniertes Payload-Profil nicht wie erwartet. Sie sollten vorhandene Richtlinien oder Profile verwenden, wann immer dies möglich ist.

Sie können mit dem Apple Apple Configurator-Konfigurationsprofile erstellen und diese den benutzerdefinierten BlackBerry UEM-Payload-Profilen hinzufügen. Sie können benutzerdefinierte Payload-Profile Benutzern, Benutzergruppen und Gerätegruppen zuweisen.

- Kontrolle einer vorhandenen iOS Funktion, die nicht in den BlackBerry UEM-Richtlinien und -Profilen enthalten ist. Mit BES10 konnte die Sekretärin der Geschäftsführung auf einem iPhone beispielsweise sowohl auf Ihr eigenes E-Mail-Konto als auch auf das des Geschäftsführers zugreifen. In BlackBerry UEM können Sie einem Gerät nur ein E-Mail-Profil zuweisen, sodass die Sekretärin also nur Zugriff auf ihr eigenes E-Mail-Konto hätte. Um dieses Problem zu lösen, können Sie ein E-Mail-Profil zuweisen, das dem iPhone der Sekretärin den Zugang zu ihrem E-Mail-Konto ermöglicht, und ein benutzerdefiniertes Payload-Profil, das dem iPhone der Sekretärin den Zugriff auf das E-Mail-Konto des Geschäftsführers ermöglicht.
- Steuerung einer neuen iOS-Funktion, die nach Veröffentlichung der neuesten Version der BlackBerry UEM-Software erschienen ist. Sie möchten beispielsweise eine neue Funktion steuern, die auf Geräten nach einem Upgrade auf das neueste iOS-Update verfügbar ist, aber BlackBerry UEM verfügt bis zur nächsten BlackBerry UEM-Softwareversion über kein Profil für die neue Funktion. Um dieses Problem zu lösen, können Sie ein benutzerdefiniertes Payload-Profil erstellen, über das sich diese Funktion bis zur nächsten BlackBerry UEM-Softwareversion steuern lässt.

Benutzerdefiniertes Payload-Profil erstellen

Bevor Sie beginnen: Laden Sie die aktuelle Version des Apple Configurator von Apple herunter, und installieren Sie sie.

1. Erstellen Sie im Apple Configurator ein Apple-Konfigurationsprofil.
2. Klicken Sie in der BlackBerry UEM-Verwaltungskonsole auf **Richtlinien und Profile**.
3. Klicken Sie auf **Benutzerdefiniert > Benutzerdefinierte Payload**.
4. Klicken Sie auf +.
5. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
6. Kopieren Sie im Apple Configurator den XML-Code für das Apple-Konfigurationsprofil. Achten Sie beim Kopieren von Text darauf, nur die Elemente zu kopieren, die wie im folgenden Codebeispiel gezeigt, in Fettdruck dargestellt werden.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
    "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
    <plist version="1.0">
    <dict>
         <key>PayloadContent</key>
         <array>
               <dict>
                    <key>CalDAVAccountDescription</key>
                    <string>CalDAV Account Description</string>
```

```
                    <key>CalDAVHostName</key>
                    <string>caldav.server.example</string>
                    <key>CalDAVPort</key>
                    <integer>8443</integer>
                    <key>CalDAVPrincipalURL</key>
                    <string>Principal URL for the CalDAV account</string>
                    <key>CalDAVUseSSL</key>
                    </true>
                    <key>CalDAVUsername</key>
                    <string>Username</string>
                    <key>PayloadDescription</key>
                    <string>Configures CalDAV account.</string>
                    <key>PayloadDisplayName</key>
                    <string>CalDAV (CalDAV Account Description)</string>
                    <key>PayloadIdentifier</key>
                    <string>.caldav1</string>
                    <key>PayloadOrganization</key>
                    <string></string>
                    <key>PayloadType</key>
                    <string>com.apple.caldav.account</string>
                    <key>PayloadUUID</key>
                    <string>9ADCF5D6-397C-4E14-848D-FA04643610A3</string>
                    <key>PayloadVersion</key>
                    <integer>1</integer>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string>Profile description.</string>
        <key>PayloadDisplayName</key>
        <string>Profile Name</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadRemovalDisallowed</key>
        <false/>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>7A5F8391-5A98-46EA-A3CF-C0D6EDC74632</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    </plist>
```

7. Fügen Sie im Feld **Benutzerdefinierte Payload** den XML-Code aus dem Apple Configurator ein.
8. Klicken Sie auf **Hinzufügen**.

Einrichten von werkseitigem Rücksetzschutz für Android Enterprise-Geräte

Sie können ein Profil für werkseitigen Rücksetzschutz für die Android Enterprise-Geräte Ihres Unternehmens einrichten, die mithilfe der Aktivierungsart Nur geschäftlicher Bereich aktiviert wurden. Mit diesem Profil können Sie ein Benutzerkonto festlegen, mit dem ein Gerät entsperrt werden kann, nachdem es auf die Werkseinstellungen zurückgesetzt wurde. Zu den Vorteilen dieses Profils gehört die Möglichkeit, ein Gerät zu entsperren, wenn der Benutzer die mit dem Gerät verknüpften Google-Anmeldeinformationen für das Konto vergessen hat oder wenn der ursprüngliche Gerätebenutzer nicht mehr in Ihrem Unternehmen ist.

Bei der Einrichtung dieses Profils für Geräte, die auf die Werkseinstellungen zurückgesetzt wurden, stehen drei Optionen zur Verfügung:

- Sie können den werkseitigen Rücksetzschutz deaktivieren, wenn Benutzer die Google-Anmeldeinformationen des letzten Benutzers, der das Gerät verwendet hat, nicht überprüfen müssen.
- Benutzer können die mit dem Gerät verknüpften Google-Anmeldeinformationen für das Konto verwenden
- Sie können die Google-Anmeldeinformationen für das Konto angeben, die der Benutzer beim Einrichten des Geräts verwenden kann

BlackBerry empfiehlt, dass Sie dieses Profil nur mit Google-Anmeldeinformationen implementieren, die von einem Administrator festgelegt wurden, nachdem Sie die Benutzererfahrung des Geräts vollständig verstanden haben.

Erstellen eines Profils für werkseitigen Rücksetzschutz

Bevor Sie beginnen: Sie müssen eine Benutzer-ID für ein Google-Konto erstellen, wenn Sie Google-Kontoanmeldeinformationen angeben möchten. Weitere Informationen finden Sie unter Abrufen einer Benutzer-ID für ein Google-Konto.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Verwaltete Geräte > Schutz > Werkseitiger Rücksetzschutz**.
2. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
3. Wählen Sie **Einstellung für werkseitigen Rücksetzschutz** aus. Wählen Sie eine der folgenden Optionen aus:
   - **Werkseitigen Rücksetzschutz deaktivieren**: Wenn Sie den werkseitigen Rücksetzschutz deaktivieren, werden Benutzer nicht zur Eingabe einer Google-Benutzer-ID aufgefordert, nachdem das Gerät auf die Werkseinstellungen zurückgesetzt wurde.
   - **Vorherige Google-Kontoanmeldedaten aktivieren und verwenden, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird**: Dies ist die Standardoption. Wenn der Benutzer das Gerät mithilfe einer nicht vertrauenswürdigen Methode auf die Werkseinstellungen zurücksetzt und vor dem Zurücksetzen ein Google-Konto auf dem Gerät vorhanden war, muss das Konto überprüft werden, nachdem das Gerät auf die Werkseinstellungen zurückgesetzt wurde. Beachten Sie, dass, wenn Ihr Unternehmen eine verwaltete Google-Kontostruktur verwendet, auf dem Gerät kein Google-Konto vorhanden ist und der werkseitige Rücksetzschutz nicht verfügbar ist.
   - **Anmeldedaten für Google-Konto aktivieren und angeben, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird**: Wenn Sie diese Option auswählen, klicken Sie auf **+** > **Manuell**, und geben Sie dann die Informationen in die Felder **E-Mail-Adresse** und **Google ID** ein. Informationen zum Abrufen Ihrer Google-Konto-ID finden Sie unter Abrufen einer Benutzer-ID für ein Google-Konto. Wenn das Gerät mithilfe einer nicht vertrauenswürdigen Methode auf die Werkseinstellungen zurückgesetzt wird, muss der Benutzer die E-Mail-Adresse und das Kennwort eingeben, die mit der E-Mail-Adresse des von Ihnen eingegebenen Google-Kontos verknüpft sind.

Beachten Sie, dass, wenn Sie diese Option auswählen und die Google-Kontoanmeldedaten angeben, die auf dem Gerät vorhandenen Google-Kontoanmeldedaten nicht mehr funktionieren.

4. Klicken Sie auf **Speichern**.

Abrufen einer Benutzer-ID für ein Google-Konto

Sie können ein vorhandenes Google-Konto verwenden oder ein Konto erstellen, das speziell für die Nutzung des werkseitigen Rücksetzschutzes vorgesehen ist. Sie müssen dann die Benutzer-ID abrufen, die Sie verwenden, wenn Sie das Profil für werkseitigen Rücksetzschutz einrichten.

1. Rufen Sie die Google-Entwicklerseite People API auf (https://developers.google.com/people/api/rest/v1/people/get).
2. Geben Sie in das Feld **resourceName** Folgendes ein: people/me
3. Geben Sie in das Feld **personalFields** Folgendes ein: metadata
4. Klicken Sie auf **Ausführen**.
5. Wählen Sie auf dem Bildschirm **Konto auswählen** ein Konto aus, mit dem Sie das Profil für werkseitigen Rücksetzschutz einrichten möchten.
6. Klicken Sie auf dem Bildschirm **Google APIs Explorer möchte auf Ihr Google-Konto zugreifen** auf **Zulassen**.
7. Auf der rechten Seite der People-ID-Seite wird die 21-stellige Benutzer-ID im Feld „ID“ angezeigt. Beachten Sie, dass die ID unter der grünen Kopfzeile mit der Zahl 200 angezeigt wird.

Reaktion des werkseitigen Rücksetzschutzes auf das Zurücksetzen des Geräts

Es gibt mehrere Möglichkeiten, ein Gerät auf die Werkseinstellungen zurückzusetzen. Je nachdem, auf welche Weise das Gerät zurückgesetzt wird, reagiert der werkseitige Rücksetzschutz unterschiedlich. Weitere Informationen zu vertrauenswürdigen und nicht vertrauenswürdigen Resets finden Sie in Artikel KB37660 unter support.blackberry.com/community.

- Die Deaktivierung des BlackBerry UEM Client wird nicht als vertrauenswürdiges Zurücksetzen angesehen, da der Gerätebenutzer nicht überprüft wird, bevor das Gerät deaktiviert wird. Daher wird der werkseitige Rücksetzschutz ausgelöst, wenn das Gerät zurückgesetzt und die Deaktivierung abgeschlossen ist.
- Das Senden des Befehls „Alle Gerätedaten löschen“ von der Verwaltungskonsole kann entweder ein vertrauenswürdiger oder ein nicht vertrauenswürdiger Reset sein. Wenn Sie beim Senden des Befehls die Option „Werkseitigen Rücksetzschutz aufheben“ auswählen, wird der werkseitige Rücksetzschutz nicht ausgelöst, wenn das Gerät zurückgesetzt wird.
- Um das Gerät von den Geräteeinstellungen zurückzusetzen, muss sich der Benutzer vor dem Zurücksetzen authentifizieren. Dies gilt als vertrauenswürdiges Zurücksetzen, und der werkseitige Rücksetzschutz wird nicht ausgelöst.
- Geräte-Bootloader-/Wiederherstellungs- oder Debugging-Tools (ADB) können verwendet werden, um das Gerät auf die Werkseinstellungen zurückzusetzen. Sie gelten als nicht vertrauenswürdig, da die Benutzeridentität vor dem Zurücksetzen auf die Werkseinstellungen nicht validiert wird. Daher wird der werkseitige Rücksetzschutz vor dem Zurücksetzen ausgelöst.

Überlegungen zur Verwendung eines Managed Google Play-Kontos bei der Einrichtung eines Profils für werkseitigen Rücksetzschutz

Wenn Ihre Organisation ein Managed Google Play-Konto verwendet, könnte für Sie im Profil für werkseitigen Rücksetzschutz die Option „Anmeldedaten für Google-Konto aktivieren und angeben, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird“ in Frage kommen, da auf den Geräten Ihres Unternehmens kein Google-Konto vorhanden ist, das Sie zum Zurücksetzen des Geräts verwenden, und dementsprechend auf dem Gerät kein werkseitiger Rücksetzschutz verfügbar ist.

Wenn Sie die Option „Anmeldedaten für Google-Konto aktivieren und angeben, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird“ verwenden möchten, sind einige Punkte zu beachten:

- Achten Sie darauf, dass Sie die 21-stellige Benutzer-ID korrekt in das Profil eingeben. Wenn diese Nummer nicht mit dem Google-Konto Ihres Unternehmens übereinstimmt, das Sie verwenden möchten, kann der werkseitige Rücksetzschutz auf dem Gerät nicht aufgehoben werden, sobald er einmal ausgelöst wurde. Weitere Informationen finden Sie unter Abrufen einer Benutzer-ID für ein Google-Konto.
- In der IT-Richtlinie für die Benutzer Ihres Unternehmens, denen Sie das Profil für werkseitigen Rücksetzschutz zuweisen, empfiehlt BlackBerry, die Option „Wiederherstellen der Werkseinstellungen zulassen“ zu deaktivieren. Durch das Löschen der Option werden die Option zum Zurücksetzen auf die Werkseinstellungen in den Geräteeinstellungen und die Schaltfläche zum Deaktivieren im BlackBerry UEM Client deaktiviert. Dadurch wird sichergestellt, dass die Benutzer nicht die Option einer nicht vertrauenswürdigen Deaktivierung im UEM Client verwenden, bei der auf dem Gerät immer der werkseitige Rücksetzschutz aktiviert wird. Wenn diese Option aktiviert ist, müssen Benutzer sich zum Zurücksetzen ihres Gerätes an den BlackBerry UEM-Administrator ihres Unternehmens wenden.
- Informieren Sie die Benutzer Ihres Unternehmens über den Vorgang beim werkseitigen Rücksetzschutz auf dem Gerät und das Verfahren zur Aufhebung des werkseitigen Rücksetzschutzes, wenn dieser auf dem Gerät ausgelöst wird. Weitere Informationen finden Sie unter Werkseitigen Rücksetzschutz von einem Gerät löschen. Der BlackBerry UEM-Administrator muss festlegen, ob Benutzer zur Aufhebung des werkseitigen Rücksetzschutzes die Kontodaten erhalten oder sich zum Entsperren des Gerätes an das Supportpersonal vor Ort wenden sollen.

Löschen des werkseitigen Rücksetzschutzes von einem Gerät

Wenn der werkseitige Rücksetzschutz auf dem Gerät ausgelöst wird, funktioniert die Enterprise-Aktivierung auf BlackBerry UEM nicht mehr. Sie müssen zuerst mit dem Out-of-the-Box-Experience von Android den werkseitigen Rücksetzschutz löschen.

1. Wenn Sie ein automatisiertes Aktivierungssystem verwenden (z. B. Zero-Touch-Registrierung oder Samsung Knox Mobile Enrollment), müssen Sie es deaktivieren, damit das Gerät das Out-of-the-Box-Experience durchläuft.
2. Sobald das Gerät mit dem Internet verbunden ist, wird der Benutzer auf dem Startbildschirm für das Android-Konto aufgefordert, die Anmeldedaten für das mit dem Gerät verknüpfte Google-Konto einzugeben. Wenn Sie im Profil für den werkseitigen Rücksetzschutz ein bestimmtes Google-Konto eingerichtet haben, muss der Benutzer die E-Mail-Adresse und das Kennwort für dieses Konto eingeben.
3. Nachdem der Benutzer die E-Mail-Adresse und das Kennwort für das Google-Konto eingegeben hat, wird er gefragt, ob dieser Benutzer dem Gerät hinzugefügt werden soll. Der Benutzer muss die Option auswählen, für das Gerät einen neuen Benutzer zu verwenden.

- Bei Geräten, die nicht von Samsung sind und keine Zero-Touch-Registrierung verwenden: Benutzer können „afw#blackberry“ oder die Anmeldedaten für das kommerzielle Google-Konto eingeben, um den BlackBerry UEM Client zu installieren und das Gerät erneut gegenüber BlackBerry UEM zu aktivieren.
- Auf Samsung-Geräten, die weder Zero-Touch-Registrierung noch Samsung Knox Mobile Enrollment verwenden: Durchlaufen Sie das Out-of-the-Box-Experience, und starten Sie das Gerät über die Geräteeinstellungen neu. Wenn das Gerät neu gestartet wird, kann es erneut gegenüber dem Unternehmen aktiviert werden.
- Geräte, die Zero-Touch-Registrierung oder Samsung Knox Mobile Enrollment verwenden: Wenn Sie ein automatisiertes Aktivierungssystem verwenden (z. B. Zero-Touch-Registrierung oder Samsung Knox Mobile Enrollment), können Sie es für das Gerät erneut aktivieren, das Out-of-the-Box-Experience durchlaufen und das Gerät über die Geräteeinstellungen zurücksetzen. Das Gerät sollte jetzt neu starten und dabei das von Ihnen konfigurierte automatische Aktivierungssystem verwenden.

Einrichten von Windows-Unternehmensdatenschutz für Windows 10-Geräte

Sie können den Windows-Unternehmensdatenschutz (WIP) für Windows 10-Geräte einrichten, wenn Sie Folgendes erreichen möchten:

- Trennen von persönlichen und geschäftlichen Daten auf Geräten mit der Möglichkeit, nur geschäftliche Daten zu löschen
- Verhindern, dass Benutzer geschäftliche Daten außerhalb der geschützten geschäftlichen Apps oder für Personen außerhalb Ihres Unternehmens freigeben
- Schützen von Daten, auch wenn diese auf andere Geräte verschoben oder auf diesen freigegeben werden, z. B. USB-Sticks
- Überwachen des Benutzerverhaltens und Ergreifen von entsprechenden Maßnahmen zur Vermeidung von Datenlecks

Wenn Sie den Unternehmensdatenschutz auf Geräten einrichten, legen Sie fest, welche Apps mit WIP geschützt werden sollen. Geschützte Apps gelten als vertrauenswürdig und können zum Erstellen von und für den Zugriff auf geschäftliche Daten genutzt werden, während der Zugriff nicht geschützter Apps auf geschäftliche Dateien gesperrt werden kann. Sie können das erforderliche Maß an Schutz für geschützte Apps basierend darauf festlegen, wie Benutzer sich bei der Freigabe von geschäftlichen Daten verhalten sollen. Wenn WIP aktiviert ist, werden alle Datenfreigabepraktiken überwacht. Weitere Informationen zu WIP finden Sie unter https://technet.microsoft.com/itpro/windows/keep-secure/protect-enterprise-data-using-wip.

Die von Ihnen angegebenen Apps können uneingeschränkt oder eingeschränkt EDP-fähig sein. Uneingeschränkt EDP-fähige Apps können geschäftliche und persönliche Daten erstellen und auf diese zugreifen. Eingeschränkt EDP-fähige Apps können nur geschäftliche Daten erstellen und auf diese zugreifen. Weitere Informationen zu uneingeschränkten und eingeschränkten Apps finden Sie unter https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/enlightened-microsoft-apps-and-wip.

Erstellen eines Windows-Datenschutzprofils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Schutz > Windows-Datenschutz**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Konfigurieren Sie die entsprechenden Werte für die jeweilige Profileinstellung. Weitere Einzelheiten zu den Profileinstellungen finden Sie unter Windows 10: Profileinstellungen für Windows-Datenschutz.
6. Klicken Sie auf **Hinzufügen**.

Windows 10: Profileinstellungen für Windows-Datenschutz

Windows 10: Profileinstellung für Windows-Datenschutz	Beschreibung
Einstellungen für Windows-Datenschutz	Diese Einstellung legt fest, ob und mit welchen Durchsetzungsmaßnahmen der Windows-Datenschutz aktiviert wird. Wenn diese Einstellung auf „Deaktiviert“ gesetzt ist, werden Daten nicht verschlüsselt, und die Audit-Protokollierung wird deaktiviert. Wenn diese Einstellung auf „Im Hintergrund“ gesetzt ist, werden Daten verschlüsselt, und alle Versuche, geschützte Daten freizugeben, werden protokolliert. Wenn hier „Außer Kraft setzen“ eingestellt ist, werden Benutzer zur Eingabe aufgefordert, wenn sie versuchen, geschützte Daten freizugeben, und Freigabeversuche werden protokolliert. Wenn diese Einstellung auf „Sperren“ gesetzt ist, werden Daten verschlüsselt, Benutzer können geschützte Daten nicht freigeben, und Freigabeversuche werden protokolliert. Mögliche Werte: • Deaktiviert • Im Hintergrund • Außer Kraft setzen • Sperren Der Standardwert ist „Aus“.
Geschützte Domänennamen im Unternehmen	Diese Einstellung legt die geschäftlichen Netzwerkdomänennamen fest, die Ihr Unternehmen für seine Benutzeridentitäten verwendet. Bei Eingabe mehrerer Domänen können senkrechte Striche (|) als Trennzeichen verwendet werden. Die erste Domäne wird als Zeichenfolge für die Kennzeichnung von Dateien verwendet, die durch Apps geschützt werden, die WIP verwenden. Beispielsweise `beispiel.com|beispiel.net`.
Zertifikatdatei zur Datenwiederherstellung (.der, .cer)	Diese Einstellung legt die für die Datenwiederherstellung verwendete Zertifikatdatei fest. Die angegebene Datei muss ein PEM- oder DER-codiertes Zertifikat mit der Dateierweiterung .der oder .cer sein. Sie verwenden die Zertifikatdatei zur Datenwiederherstellung zur Wiederherstellung von lokal geschützten Dateien auf einem Gerät. Beispielsweise wenn Ihr Unternehmen durch WIP geschützte Daten eines Geräts wiederherstellen möchte. Weitere Informationen zum Erstellen eines Datenwiederherstellungszertifikats finden Sie in der Microsoft Windows Datenschutz-Dokumentation.
Windows-Datenschutzeinstellungen entfernen, wenn ein Gerät aus BlackBerry UEM entfernt wird	Diese Einstellung legt fest, ob die WIP-Einstellungen gesperrt werden, sobald ein Gerät deaktiviert wird. Wenn die WIP-Einstellungen gesperrt werden, kann der Benutzer nicht mehr auf geschützte Dateien zugreifen.

Windows 10: Profileinstellung für Windows-Datenschutz	Beschreibung
Symboleinblendungen für Windows-Datenschutz in geschützten Dateien und Apps anzeigen, die Unternehmensinhalte erstellen können	Diese Einstellung legt fest, ob auf den Datei- und App-Symbolen eine Einblendung angezeigt wird, die angibt, ob die Datei oder App durch WIP geschützt ist.
IP-Bereich des geschäftlichen Netzwerks	Diese Einstellung legt den geschäftlichen IP-Adressbereich fest, an den eine mit WIP geschützte Datei Daten freigeben kann. Die Adressbereiche können mit einem Gedankenstrich gekennzeichnet werden. Adressen können mit einem Komma voneinander abgegrenzt werden.
IP-Bereiche des geschäftlichen Netzwerks sind verbindlich	Diese Einstellung legt fest, ob nur die IP-Bereiche des geschäftlichen Netzwerks als Teil des geschäftlichen Netzwerks akzeptiert werden. Wenn diese Einstellung aktiviert ist, werden keine Versuche unternommen, weitere geschäftliche Netzwerke zu erkennen. Diese Option ist standardmäßig deaktiviert.
Interne Proxyserver des Unternehmens	Diese Einstellung legt die internen Proxyserver fest, die für Verbindungen zu Standorten des Geschäftsnetzwerks verwendet werden. Diese Proxyserver werden nur verwendet, wenn eine Verbindung mit der Domäne hergestellt wird, die in der Einstellung „Enterprise-Cloud-Ressourcen“ aufgeführt ist.
Cloud-Unternehmensressourcen	Diese Einstellung legt die Liste der in der Cloud gehosteten Domänen mit Unternehmensressourcen fest, die geschützt werden müssen. Daten von diesen Ressourcen gelten als zu schützende Unternehmensdaten.
Cloud-Ressourcendomäne	Diese Einstellung legt den Domänennamen fest.
Gekoppelter Proxy	Diese Einstellung legt den Proxy fest, der mit einer Cloud-Ressource gekoppelt ist. Der Datenverkehr zur Cloud-Ressource wird über den angegebenen Proxyserver (an Port 80) durch das Unternehmensnetzwerk geleitet. Ein zu diesem Zweck verwendeter Proxyserver muss auch im Feld für die internen Proxyserver des Unternehmens konfiguriert werden.
Enterprise-Proxy-Server	Diese Einstellung gibt die Liste der Internet-Proxyserver an.
Enterprise-Proxy-Server sind erforderlich	Diese Einstellung gibt an, ob der Client die konfigurierte Liste der Proxys akzeptieren und nicht versuchen soll, andere Enterprise-Proxys zu erkennen.
Neutrale Ressourcen	Diese Einstellung legt die Domänen fest, die für geschäftliche oder persönliche Ressourcen verwendet werden können.

Windows 10: Profileinstellung für Windows-Datenschutz	Beschreibung
Domänennamen im Unternehmensnetzwerk	Diese Einstellung legt eine durch Komma getrennte Liste von Domänen fest, die die Grenzen des Unternehmens darstellen. An ein Gerät gesendete Daten aus diesen Domänen gelten als Unternehmensdaten und werden geschützt. Diese Standorte gelten als sicheres Ziel, für das Unternehmensdaten freigegeben werden dürfen. Z. B. `beispiel.com,beispiel.net`.

Payload-Code für Desktop-App	Geben Sie die Schlüssel und Werte der Desktop-App zur Konfiguration der Beschränkungen für den Anwendungsstart auf Windows 10-Geräten ein. Sie müssen die von Microsoft festgelegten Schlüssel für die zu konfigurierende Payload-Art verwenden.
	
	Um die Apps anzugeben, kopieren Sie den XML-Code der Datei „AppLocker policy.xml“, und fügen Sie ihn in dieses Feld ein. Achten Sie beim Kopieren von Text darauf, nur die Elemente wie im folgenden Codebeispiel gezeigt zu kopieren.
	
	`<RuleCollection Type="Appx" EnforcementMode="Enabled">
	  <FilePublisherRule Id="0c9781aa-bf9f-4352-b4ba-64c25f36f558"
	  Name="WordMobile" Description="
	 UserOrGroupSid="S-1-1-0" Action="Allow">
	  <Conditions>
	  <FilePublisherCondition
	  PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US"
	  ProductName="Microsoft.Office.Word" BinaryName="*">
	  <BinaryVersionRange LowSection="*" HighSection="*" />
	  </FilePublisherCondition>
	  </Conditions>
	  </FilePublisherRule>
	</RuleCollection>`
	
	Weitere Informationen zu AppLocker finden Sie in der Microsoft AppLocker-Dokumentation.

Windows 10: Profileinstellung für Windows-Datenschutz	Beschreibung

Payload-Code für universelle Windows-Plattform-App	Geben Sie die Schlüssel und Werte der universellen Windows-Plattform-App zur Konfiguration von WIP auf Windows 10-Geräten ein. Sie müssen die von Microsoft festgelegten Schlüssel für die zu konfigurierende Payload-Art verwenden.
	
	Um die Apps anzugeben, kopieren Sie den XML-Code der Datei „AppLocker policy.xml“, und fügen Sie ihn in dieses Feld ein. Achten Sie beim Kopieren von Text darauf, nur die Elemente wie im folgenden Codebeispiel gezeigt zu kopieren.
	
	`<RuleCollection Type="Exe" EnforcementMode="Enabled">`
	`  <FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20"`
	`  Name="(Default Rule)`
	`  All files" Description="" UserOrGroupSid="S-1-1-0"`
	`  Action="Allow">`
	`  <Conditions>`
	`  <FilePathCondition Path="*" />`
	`  </Conditions>`
	`  </FilePathRule>`
	`  <FilePublisherRule Id="ddd0bc90-`
	`dada-4002-9e2f-0fc68e1f6af0" Name="WORDPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Deny">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="WORDPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`  <FilePublisherRule Id="c8360d06-f651-4883-`
	`abdd-9c3a95a415ff" Name="NOTEPAD.EXE,`
	`  from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`  C=US" Description=""`
	`  UserOrGroupSid="S-1-1-0" Action="Allow">`
	`  <Conditions>`
	`  <FilePublisherCondition PublisherName="O=MICROSOFT`
	`  CORPORATION,`
	`  L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`  BinaryName="NOTEPAD.EXE">`
	`  <BinaryVersionRange LowSection="*"`
	`  HighSection="*" />`
	`  </FilePublisherCondition>`
	`  </Conditions>`
	`  </FilePublisherRule>`
	`</RuleCollection>`
	
	Weitere Informationen zu AppLocker finden Sie in der Microsoft AppLocker-Dokumentation.

Windows 10: Profileinstellung für Windows-Datenschutz	Beschreibung
Verknüpftes VPN-Profil	Diese Einstellung legt das verknüpfte VPN-Profil fest, das ein Gerät verwendet, um eine Verbindung zu einem VPN aufzubauen, wenn eine App mit WIP-Schutz verwendet wird. Diese Einstellung ist nur gültig, wenn „Ein VPN-Profil verwenden“ für „Verwendete Verbindung mit WIP schützen“ ausgewählt ist.
Überwachungsprotokolle für das Gerät erfassen	Diese Einstellung legt fest, ob Überwachungsprotokolle für das Gerät erfasst werden sollen.

Zulassen der BitLocker-Verschlüsselung auf Windows 10-Geräten

BitLocker Drive Encryption ist eine Datenschutzfunktion des Betriebssystems, die bei Verlust oder Diebstahl eines Geräts den unbefugten Zugriff auf Daten verhindert. Sie können die BitLocker-Verschlüsselung auf Windows 10-Geräten zulassen. Wenn das Gerät zusätzlich über ein TPM (Trusted Platform Module) verfügt, das Ihnen die Möglichkeit bietet, beim Start eine zusätzliche Authentifizierung anzufordern (z. B. Startschlüssel, PIN oder USB-Wechseldatenträger) kann die Verschlüsselung noch verstärkt werden. In BlackBerry UEM können Sie zudem ein Konformitätsprofil erstellen, das verhindert, dass Benutzer BitLocker deaktivieren, und so die Verwendung auf Geräten, die eine Verschlüsselung erfordern, durchsetzen.

Sie können die Wiederherstellungsoptionen für den Zugriff auf ein mit BitLocker geschütztes Betriebssystem oder Datenlaufwerke konfigurieren. Benutzer können von der Active Directory-Konsole aus auf Wiederherstellungsschlüssel zugreifen. Wenn diese Option aktiviert ist, können Wiederherstellungskennwörter in den Active Directory-Domänendiensten gesichert und von einem Administrator mit dem Tool BitLocker-Wiederherstellungskennwort-Viewer wiederhergestellt werden.

Konfigurieren Sie die folgenden UEM-IT-Richtlinienregeln zur Unterstützung der BitLocker-Verschlüsselung auf Windows 10-Geräten:

- BitLocker-Verschlüsselungsmethode für Desktop
- Eingabeaufforderungen zur Speicherkartenverschlüsselung auf dem Gerät zulassen
- BitLocker Device Encryption kann Verschlüsselung auf dem Gerät aktivieren
- Standard-Verschlüsselungsmethoden für jeden Laufwerkstyp festlegen
- Zusätzliche Authentifizierung beim Start erforderlich
- Mindestlänge der PIN für den Start erforderlich
- Pre-Boot-Wiederherstellungsmeldung und URL
- BitLocker-Wiederherstellungsoptionen für Betriebssystemlaufwerke
- BitLocker-Wiederherstellungsoptionen für Festplattenlaufwerke
- BitLocker-Schutz für Festplatten-Datenlaufwerke erforderlich
- BitLocker-Schutz für Wechseldatenträger erforderlich
- Eingabeaufforderung für Speicherort des Wiederherstellungsschlüssels zulassen. Verschlüsselung für Standardbenutzer aktivieren

Weitere Informationen zu den BitLocker-IT-Richtlinienregeln finden Sie in der Richtlinien-Referenztabelle.

Verwalten von Nachweisen für Geräte

Wenn Sie Nachweise aktivieren, sendet BlackBerry UEM Anforderungen zum Testen der Authentizität und Integrität von Geräten. Sie können Nachweise für die folgenden Geräte aktivieren:

- Samsung Knox-Geräte
- Android-Geräte
- Windows 10-Geräte

Verwalten von Nachweisen für Samsung Knox-Geräte

Wenn Sie Nachweise aktivieren, sendet BlackBerry UEM Anforderungen zum Testen der Authentizität und der Integrität von Samsung Knox-Geräten, die mit den folgenden Aktivierungsarten aktiviert wurden:

- Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)
- Nur geschäftlicher Bereich (Samsung Knox)
- Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Nachweis**.
2. Um Nachweise für Samsung Knox-Geräte zu aktivieren, wählen Sie **Regelmäßige Nachweisabfragen für KNOX Workspace-Geräte aktivieren** aus.
3. Geben Sie im Abschnitt **Abfragehäufigkeit** in Tagen oder Stunden an, wie oft das Gerät eine Nachweisantwort an BlackBerry UEM senden muss.
4. Geben Sie im Abschnitt **Übergangsfrist** eine Übergangsfrist in Stunden oder Tagen an. Nach Ablauf der Übergangsfrist ohne erfolgreiche Nachweisantwort wird ein Gerät als nicht konform betrachtet. Es unterliegt dann den Bedingungen des Konformitätsprofils, das diesem Benutzer zugewiesen wurde. Wenn sich das Gerät eines Benutzers außerhalb der Mobilfunkabdeckung befindet, ausgeschaltet ist oder der Akku leer ist, kann es nicht auf die Nachweisabfragen antworten, die von BlackBerry UEM gesendet werden, und BlackBerry UEM stuft das Gerät als nicht konform ein. Wenn Sie die Konformitätsrichtlinie Ihres Unternehmens so festgelegt haben, dass das Gerät bereinigt wird, wenn es nicht richtlinienkonform ist und nicht reagiert, bevor die Übergangsfrist abgelaufen ist, werden die Daten auf dem Gerät gelöscht.
5. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Erstellen Sie ein Compliance-Profil, in dem die Schritte aufgeführt sind, die durchgeführt werden, wenn ein Gerät als „gehackt“ betrachtet wird. Anweisungen finden Sie unter Durchsetzen von Kompatibilitätsregeln für Geräte

Verwalten des Nachweises für Android-Geräte und BlackBerry Dynamics-Apps mit SafetyNet

Wenn Sie Android SafetyNet-Nachweise verwenden, sendet BlackBerry UEM Abfragen zum Testen der Authentizität und der Integrität von Android-Geräten und BlackBerry Dynamics-Apps in der Umgebung Ihres Unternehmens. SafetyNet hilft Ihnen, die Sicherheit und Kompatibilität der Umgebungen zu bewerten, in denen die Apps Ihres Unternehmens ausgeführt werden. Sie können den SafetyNet-Nachweis neben der bestehenden Root- und Exploit-Erkennung von BlackBerry verwenden. Weitere Informationen zu SafetyNet finden Sie in den Informationen von Google.

Die folgenden Produkte unterstützen den SafetyNet-Nachweis:

- BlackBerry UEM

- BlackBerry UEM Client für Android
- BlackBerry Dynamics-Apps für Android

Überlegungen zur Konfiguration des SafetyNet-Nachweises

- Die Option „Nachweisfehler für Google SafetyNet“ ist eine Konformitäts-Profileinstellung für Android-Geräte und BlackBerry Dynamics-Apps, mit der Sie die Aktionen festlegen können, die auftreten, wenn Geräte oder Apps den Nachweis nicht bestehen.SafetyNet. Um diese Option einzustellen, navigieren Sie zu der Registerkarte **Richtlinien und Profile > Konformität > Android**.
- Wenn Sie die Konformitätsregel „Nachweisfehler Google SafetyNet“ nicht aktivieren, werden bereits aktivierte Apps nicht mit Konformitätsaktionen belegt.
- Wenn Sie SafetyNet aktivieren, wird der Nachweis während der Aktivierung durchgeführt; Sie können eine Richtlinie nicht verwenden, um einen Nachweis während der Aktivierung durchzusetzen.
- BlackBerry UEM Client ist nicht erforderlich, um den SafetyNet-Nachweis zu aktivieren.
- BlackBerry UEM Client wird nicht in der Liste der BlackBerry Dynamics-Apps angezeigt, die Sie für den SafetyNet-Nachweis konfigurieren können. BlackBerry UEM sendet Nachweisabfragen an und erhält Antworten von BlackBerry UEM Client.
- BlackBerry UEM sendet Nachweisabfragen an jede BlackBerry Dynamics-App, die Sie konfigurieren.
- BlackBerry UEM behandelt alte Versionen der Apps nicht als vertrauenswürdig. Wenn Sie zum Beispiel Nachweisabfragen für BlackBerry Work aktivieren möchten, müssen Sie sicherstellen, dass die Version von BlackBerry Work auf den Geräten Ihres Unternehmens die neueste Version ist, andernfalls schlagen neue Aktivierungen fehl. Beachten Sie, dass bis zur Aktivierung der Option „Nachweisfehler Google SafetyNet“ im Konformitätsprofil Ihres Unternehmens, keine nachteiligen Maßnahmen für Apps oder Geräte ergriffen werden, selbst wenn die bestehenden aktivierten Benutzer ältere Appversionen verwenden.
- Neben der Aktivierung und dem regelmäßigen Nachweis nutzt BlackBerry UEM neue REST-APIs, mit denen Sie benutzerdefinierte Server-Workflows erstellen können. Wenn eine App beispielsweise auf ein bestimmtes sicheres Remote-Element zugreifen muss, kommuniziert der App-Server vor der Gewährung des Zugriffs mit BlackBerry UEM, um den SafetyNet-Nachweis auf der App oder dem Gerät durchzusetzen.
- Wenn sich das Gerät eines Benutzers außerhalb der Mobilfunkabdeckung befindet, ausgeschaltet ist oder der Akku leer ist, kann es nicht auf die Nachweisabfragen antworten, die von BlackBerry UEM gesendet werden, und BlackBerry UEM stuft das Gerät als nicht konform ein. Wenn Sie die Konformitätsrichtlinie Ihres Unternehmens so festgelegt haben, dass das Gerät bereinigt wird, wenn es nicht richtlinienkonform ist und nicht reagiert, bevor die Übergangsfrist abgelaufen ist, werden die Daten auf dem Gerät bei der Verbindung mit einem Drahtlosnetzwerk gelöscht.
- Wenn Sie im Feld „App-Übergangsfrist“ eine Zeit festlegen, wird nur für die Apps, die nicht innerhalb des von Ihnen festgelegten Zeitrahmens antworten, eine Aktion durchgeführt. Wenn Sie den Wert im Feld „App-Übergangsfrist“ beispielsweise auf 7 Tage setzen und Ihre Benutzer BlackBerry Work jeden Tag nutzen, aber BlackBerry Tasks nicht innerhalb der 7 Tage nutzen, wird nur für BlackBerry Tasks eine Aktion ausgeführt.
- Wenn Sie eine neue App zu BlackBerry UEM hinzufügen und der Nachweis während der Aktivierung fehlschlägt, wird die App nicht aktiviert, unabhängig davon, welche Option Sie im Abschnitt „Nachweisfehler Google SafetyNet“ des Konformitätsprofils Ihres Unternehmens konfiguriert haben. Wenn eine App bereits aktiviert wurde, unterliegt sie den Regeln, die Sie im Konformitätsprofil angegeben haben.
- Die Benutzer in Ihrem Unternehmen müssen die neueste Version der Google Play-Dienste installiert haben.
- Wenn der Nachweis für ein Gerät fehlschlägt, gibt es keinen Hinweis auf den Fehler in der Spalte „Betroffenes Betriebssystem“ auf der Seite „Verwaltete Geräte“.
- Weitere Informationen über das Entwickeln von BlackBerry Dynamics-Apps für Android-Geräte finden Sie im Abschnitt Entwickler.

Überlegungen zur Konfiguration des SafetyNet-Nachweises – App-Versionen

- Bevor Sie den SafetyNet-Nachweis für die Android-Geräte Ihres Unternehmens aktivieren, stellen Sie sicher, dass die Benutzer des Geräts UEM Client auf ihren Geräten auf Version 12.9 MR1 oder höher aktualisiert haben, anderenfalls werden die Aktionen zur Einhaltung der Übergangsfrist auf dem Gerät durchgesetzt.
- Wenn Sie den Nachweis für die BlackBerry UEM-Instanz Ihres Unternehmens aktivieren und Sie BlackBerry UEM Client-Version 12.10 installiert haben, wird bei der Android-Geräteaktivierung die Authentizität und Integrität des Geräts überprüft. Wenn Sie BlackBerry UEM Client-Version 12.9 MR1 installiert haben, wird der SafetyNet-Nachweis auf Geräteebene nach der Aktivierung durchgeführt. Stellen Sie sicher, dass Sie BlackBerry UEM Client für Android-Version 12.9 MR1 oder höher auf den Android-Geräten in Ihrem Unternehmen installiert haben, bevor Sie die Funktion aktivieren.

Version von BlackBerry UEM	Wann der SafetyNet-Nachweis durchgeführt wird
12.9 MR1	Nach der Geräteaktivierung
12.10, 12.11, 12.12	• Nach der Geräteaktivierung, wenn BlackBerry UEM Client installiert ist • Während der Geräteaktivierung, wenn BlackBerry UEM Client installiert ist • Während der Aktivierung der BlackBerry Dynamics-Apps • Nach der App-Aktivierung für BlackBerry Dynamics-Apps • Nach Bedarf mithilfe von REST-APIs • Beim Neustart des Geräts, wenn BlackBerry UEM Client aktiviert ist

- Wenn Sie BlackBerry UEM 12.9 MR1 in der Umgebung Ihres Unternehmens installiert haben und den SafetyNet-Nachweis aktiviert haben, müssen Sie beim Upgrade auf BlackBerry UEM12.10 die Option „Nachweisfehler Google SafetyNet“ im Konformitätsprofil Ihres Unternehmens auswählen, damit die Android-Geräte Ihres Unternehmens den Durchsetzungsaktionen des SafetyNet-Nachweises nicht unterliegen.

Verwalten des Nachweises für Android-Geräte und BlackBerry Dynamics-Apps mit SafetyNet

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Nachweis**.
2. Um Nachweise für Android-Geräte zu aktivieren, wählen Sie **Regelmäßige Nachweisabfragen mithilfe von SafetyNet aktivieren** aus.
3. Wählen Sie **CTS-Profilanpassung aktivieren** aus, wenn Sie die Compatibility Test Suite von Google einschalten wollen. Weitere Informationen zu CTS finden Sie in den Informationen von Google.
4. Geben Sie im Abschnitt **Abfragehäufigkeit** in Tagen oder Stunden an, wie oft das Gerät eine Nachweisantwort an BlackBerry UEM senden muss. Überlegungen zur Konfiguration der Abfragehäufigkeit:
   - Sie können zwar konfigurieren, wie oft BlackBerry UEM die Authentizität und Integrität des Geräts überprüft, der Nachweis während der Aktivierung der App ist jedoch obligatorisch.
   - Wenn Sie den BlackBerry UEM Client bereitgestellt haben, wird er als eine der Apps hinzugefügt, die BlackBerry UEM automatisch den SafetyNet-Nachweis überprüft.
   - BlackBerry UEM Client verwendet einen anderen Kommunikationskanal zu BlackBerry UEM als andere BlackBerry Dynamics-Apps, die ausgeführt werden müssen und über die Berechtigung verfügen müssen, eine Verbindung zu BlackBerry UEM herzustellen, um Richtlinienaktualisierungen zu erhalten. BlackBerry UEM kann proaktiv mit dem BlackBerry UEM Client kommunizieren und die App starten, wenn sie nicht ausgeführt wird. Wenn Sie eine Abfragehäufigkeit von 3 Stunden festlegen, dann kommuniziert BlackBerry UEM alle 3 Stunden mit dem BlackBerry UEM Client, und die Nachweisprüfung wird durchgeführt. BlackBerry Dynamics-App-Befehle werden jedoch gespeichert, bis die App eine Verbindung zu BlackBerry

UEM herstellt, und nur der neueste Nachweisbefehl wird gespeichert. Wenn die App also 24 Stunden lang nicht verwendet wird und der Benutzer sie startet, wird nur eine Nachweisaufforderung ausgeführt.

5. Geben Sie im Abschnitt **Übergangsfrist** eine Übergangsfrist in Stunden oder Tagen an. Nach Ablauf der Übergangsfrist ohne erfolgreiche Nachweisantwort wird ein Gerät als nicht konform betrachtet. Es unterliegt dann den Bedingungen des Konformitätsprofils, das diesem Benutzer zugewiesen wurde. Wenn sich das Gerät eines Benutzers außerhalb der Mobilfunkabdeckung befindet, ausgeschaltet ist oder der Akku leer ist, kann es nicht auf die Nachweisabfragen antworten, die von BlackBerry UEM gesendet werden, und BlackBerry UEM stuft das Gerät als nicht konform ein. Wenn Sie die Konformitätsrichtlinie Ihres Unternehmens so festgelegt haben, dass das Gerät bereinigt wird, wenn es nicht richtlinienkonform ist und nicht reagiert, bevor die Übergangsfrist abgelaufen ist, werden die Daten auf dem Gerät bei der Verbindung mit einem Drahtlosnetzwerk gelöscht.
6. Geben Sie im Abschnitt **App-Übergangsfrist** eine Übergangsfrist in Stunden oder Tagen an. Nach Ablauf der Übergangsfrist unterliegen BlackBerry Dynamics-Apps den Bedingungen des Konformitätsprofils, das diesem Benutzer zugewiesen wurde. Die Übergangsfrist wird pro App erzwungen. Beachten Sie, dass die Übergangsfrist ignoriert wird, wenn Sie dem Gerät nur den BlackBerry UEM Client bereitgestellt haben. Außerdem wird der BlackBerry UEM Client nicht in der Liste der BlackBerry Dynamics-Apps angezeigt. Wenn Sie BlackBerry Dynamics-Apps zur Liste der Apps hinzufügen, die den Nachweisabfragen unterliegen, gelten die folgenden Regeln:
   - Nur für Apps in dieser Liste werden Nachweisabfragen gesendet.
   - Nur Apps in dieser Liste werden für die Überprüfung der App-Übergangsfrist bewertet.
   - Nur Apps in dieser Liste unterliegen dem Nachweis während der App-Aktivierung.

   Hinweis: Nur BlackBerry Dynamics-Apps, die speziell für SafetyNet entwickelt wurden, werden in der Liste angezeigt. Weitere Informationen finden Sie in der Dokumentation für Entwickler.
7. Um eine App hinzuzufügen, die den Nachweisabfragen unterliegt, klicken Sie auf +.
8. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Namen einer App, die bereits in der Liste enthalten ist.
   - Suchen Sie nach dem Namen der App, und klicken Sie darauf.
9. Klicken Sie auf **Auswählen**.
10. Klicken Sie auf **Speichern**.

Verwalten von Nachweisen für Windows 10-Geräte

Wenn Sie den Nachweis aktivieren, sendet BlackBerry UEM Abfragen zum Testen der Authentizität und Integrität der Windows 10-Geräte. Das Gerät kommuniziert mit dem Microsoft Health Attestation-Dienst, um die Konformität basierend auf Einstellungen zu prüfen, die Sie im Konformitätsprofil Ihres Unternehmens festlegen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Nachweis**.
2. Um Nachweise für Windows 10-Geräte zu aktivieren, wählen Sie **Regelmäßige Nachweisabfragen für Windows 10-Geräte aktivieren** aus.
3. Geben Sie im Abschnitt **Abfragehäufigkeit** in Tagen oder Stunden an, wie oft das Gerät eine Nachweisantwort an BlackBerry UEM senden muss.
4. Geben Sie im Abschnitt **Übergangsfrist** eine Übergangsfrist in Stunden oder Tagen an. Nach Ablauf der Übergangsfrist ohne erfolgreiche Nachweisantwort wird ein Gerät als nicht konform betrachtet. Es unterliegt dann den Bedingungen des Konformitätsprofils, das diesem Benutzer zugewiesen wurde. Wenn sich das Gerät eines Benutzers außerhalb der Mobilfunkabdeckung befindet, ausgeschaltet ist oder der Akku leer ist, kann es nicht auf die Nachweisabfragen antworten, die von BlackBerry UEM gesendet werden, und BlackBerry UEM stuft das Gerät als nicht konform ein. Wenn Sie die Konformitätsrichtlinie Ihres Unternehmens so

festgelegt haben, dass das Gerät bereinigt wird, wenn es nicht richtlinienkonform ist und nicht reagiert, bevor die Übergangsfrist abgelaufen ist, werden die Daten auf dem Gerät gelöscht.

5. Klicken Sie auf **Speichern**.

Sie können alle Konformitätsverstöße auf der Seite „Gerätedetails“ anzeigen.

Wenn Sie fertig sind: Erstellen Sie ein Compliance-Profil, in dem die Schritte aufgeführt sind, die durchgeführt werden, wenn ein Gerät als „gehackt“ betrachtet wird. Anweisungen finden Sie unter Durchsetzen von Kompatibilitätsregeln für Geräte

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