BlackBerry UEM

Verwaltung

Verwalten von Gerätekonfigurationen

12.19

Inhalt

Verwalten von Gerätekonfigurationen

Dieses Handbuch enthält Anweisungen zur Verwendung von BlackBerry UEM-Profilen, IT-Richtlinien und anderen wichtigen Funktionen zur Konfiguration von Arbeitsgeräten gemäß den Bedürfnissen und Sicherheitsanforderungen Ihres Unternehmens.

Aufgabe	Beschreibung
Verwenden von Profilen zur Verwaltung von Gerätefunktionen.	Konfigurieren und weisen Sie Benutzern und Gruppen UEM-Profile zu, um eine Vielzahl von Gerätefunktionen und -Fähigkeiten für alle Gerätetypen zu verwalten.
Verwenden von Variablen in Profilen, E-Mails und Benachrichtigungen.	Verwenden Sie Variablen in Profilen, Benachrichtigungen zur Vorschrifteneinhaltung, Aktivierungs-E-Mails und Ereignisbenachrichtigungen, um Konfigurationen und Nachrichten für einzelne Benutzer anzupassen.
Verwenden von E-Mail-Vorlagen, um Nachrichten an Benutzer zu senden.	Verwenden Sie E-Mail-Vorlagen, um E-Mail-Nachrichten anzupassen und zu personalisieren, die UEM aus verschiedenen Gründen an Benutzer sendet, einschließlich Anweisungen zur Geräteaktivierung, Benachrichtigung von Benutzern über Konformitätsprobleme und Bereitstellung von Zugriffsschlüsseln für BlackBerry Dynamics-Apps.
Verwalten von Geräten mit IT-Richtlinien.	Verwenden Sie IT-Richtlinien, um Gerätefunktionen und -funktionalität zu steuern. Sie können beispielsweise IT-Richtlinienregeln verwenden, um Kennwortanforderungen durchzusetzen, die Verwendung bestimmter Gerätefunktionen (z. B. der Kamera) zu verhindern und die Verfügbarkeit bestimmter Apps zu steuern.
Erstellen von Geräte-Supportmeldungen für deaktivierte Funktionen auf Android-Geräten.	Lassen Sie eine Supportmeldung auf Android-Geräten anzeigen, wenn eine Funktion durch eine IT-Richtlinie deaktiviert ist.
Durchsetzen von Konformitätsregeln für Geräte.	Verwenden Sie Konformitätsprofile, um Benutzer zu ermutigen, die Gerätestandards Ihres Unternehmens zu befolgen. Ein Konformitätsprofil definiert die Gerätebedingungen, die in Ihrem Unternehmen nicht akzeptabel sind, und legt die Erzwingungsaktionen für UEM fest, die ausgeführt werden müssen, wenn der Benutzer Konformitätsprobleme nicht berichtigt.
Senden von Befehlen an Benutzer und Geräte.	Sie können verschiedene Befehle senden, um Benutzerkonten und -geräte zu verwalten. Sie können beispielsweise einen Befehl senden, um ein Gerät zu sperren oder alle geschäftlichen Daten von einem Gerät zu löschen.
Steuern, wie Softwareupdates auf Geräten installiert werden.	Verwenden Sie die Profile für Gerätedienstanforderungen, um zu steuern, wie Softwareupdates für Geräte auf Geräten installiert werden.
Konfigurieren, wie Geräte UEM kontaktieren, um App- und Konfigurationsaktualisierungen zu erhalten.	Verwenden Sie Enterprise Management Agent-Profile, um zu konfigurieren, wie Geräte Kontakt zu UEM für App- oder Konfigurationsaktualisierungen aufnehmen.

Aufgabe	Beschreibung
Anzeigen von Unternehmensinformationen auf Geräten.	Verwenden Sie Organisationshinweise und Geräteprofile, um Unternehmensinformationen auf Geräten anzuzeigen.
Verwenden von Standortdiensten auf Geräten.	Verwenden Sie Profile für die Standortbestimmung, um den Standort von Geräten anzufordern und deren ungefähre Position auf einer Karte anzuzeigen.
Aktivieren der Aktivierungssperre für ein iOS-Gerät.	Verwenden Sie die Aktivierungssperre auf iOS-Geräten, damit Benutzer ihre verlorenen oder gestohlenen Geräte schützen können. 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.
Verwalten von iOS-Funktionen mit benutzerdefinierten Payload-Profilen.	Verwenden Sie benutzerdefinierte Payload-Profile, um Funktionen auf iOS-Geräten zu steuern, die nicht durch bestehende UEM-Richtlinien oder -Profile gesteuert werden.
Verwalten des werkseitigen Rücksetzschutzes für Android-Geräte.	Verwenden Sie Profile für werkseitigen Rücksetzschutz, um die Funktion für werkseitigen Rücksetzschutz für die Android Enterprise- und Android Management-Geräte Ihres Unternehmens zu steuern.
Konfigurieren von Nachweisen für Geräte.	Senden Sie Anforderungen zum Testen der Authentizität und Integrität von Samsung Knox-, Android- und Windows 10-Geräten.
Einrichten von Windows-Datenschutz für Windows 10-Geräte.	Verwenden Sie Windows-Datenschutzprofile, um geschäftliche Daten auf Windows 10-Geräten zu schützen und zu verwalten.
Verschieben von iOS- oder macOS-Geräten in einen gehärteten Kanal.	Wenn Sie iOS- oder macOS-Geräte aktivieren, werden die Geräte standardmäßig einem gehärteten Datenkanal zugewiesen. Wenn Sie iOS- oder macOS-Geräte haben, die derzeit keinen gehärteten Datenkanal verwenden, können Sie eine Liste dieser Geräte exportieren und Maßnahmen ergreifen, um die Geräte in einen gehärteten Kanal zu verschieben.

Verwenden von Profilen zur Verwaltung von Gerätefunktionen

BlackBerry UEM verwendet verschiedene Profiltypen, um eine Vielzahl von Gerätefunktionen und Fähigkeiten für iOS-, macOS-, Android- und Windows-Geräte zu verwalten. Sie konfigurieren ein Profil entsprechend der Anforderungen Ihres Unternehmens und weisen es dann Benutzerkonten, Benutzergruppen und Gerätegruppen zu, um diese Konfiguration auf Geräte anzuwenden.

Eine vollständige Liste der verfügbaren Profile können Sie in der BlackBerry UEM-Profile anzeigen lassen.

Profilen kann eine Rangfolge zugewiesen sein oder nicht. UEM weist bei Profilen mit Rangfolge ein Profil dieses Typs einem Gerät zu (z. B. ein Konformitätsprofil). Wenn ein Profil mit Rangfolge direkt einem Benutzer zugewiesen wird, hat es Vorrang vor allen Profilen dieses Typs, die Benutzergruppen zugewiesen sind, zu denen der Benutzer gehört. Wenn ein Benutzer mehreren Benutzergruppen mit unterschiedlichen Profilen dieses Typs zugeordnet ist, wird anhand der Rangfolge ermittelt, welches Profil zugewiesen werden soll. Wenn das Gerät eines Benutzers zu einer Gerätegruppe gehört, hat das der Gerätegruppe zugewiesene Profil Vorrang vor demselben Profil dieses Typs, das dem Benutzer direkt zugewiesen ist. Wenn das Gerät Mitglied mehrerer Gerätegruppen mit unterschiedlichen Profilen dieses Typs ist, wird anhand einer Rangfolge festgelegt, welches Profil zugewiesen wird.

Bei Profilen ohne Rangfolge kann mehr als ein Profil dieses Typs einem Gerät zugewiesen werden, entweder über die direkte Zuweisung zu einem Benutzerkonto oder über die Gruppenzuweisung (z. B. kann einem Gerät mehr als ein Wi-Fi-Profil zugewiesen werden).

Bei bestimmten Profiltypen muss ein Profil Geräten zugewiesen werden. Wenn ein Profil nicht direkt oder über die Gruppenmitgliedschaft Benutzern zugewiesen wird, weist UEM ein vorkonfiguriertes Standardprofil zu. UEM hat ein Standard-Aktivierungsprofil, Standard-Konformitätsprofil, Standardprofil für Enterprise-Konnektivität und Standard-Enterprise Management Agent-Profil.

BlackBerry UEM-Profile

Profilname	Beschreibung	Unterstützte Gerätetypen	Mit Rang oder ohne Rang	Weitere Informationen unter
Richtlinie				
Knox Service Plugin	Einrichten und Konfigurieren des Knox Service Plugin.	Android	Mit Rang	Verwalten von Android-Geräten mit OEM-App-Konfigurationen
Aktivierung	Konfigurieren der Geräteaktivierungseinstellungen für Benutzer (z. B. die Aktivierungsart sowie die Anzahl und Gerätetypen).	Alle Geräte	Mit Rang	Erstellen von Aktivierungsprofilen

Profilname	Beschreibung	Unterstützte Gerätetypen	Mit Rang oder ohne Rang	Weitere Informationen unter
BlackBerry Dynamics	Aktivieren von BlackBerry Dynamics für Benutzer und Konfigurieren von Standards für App-Zugriff, Datenschutz und Protokollierung.	Alle Geräte	Mit Rang	Steuern von BlackBerry Dynamics auf Geräten
App-Sperrmodus	Konfigurieren eines Gerätes, um nur die von Ihnen angegebenen Apps auszuführen.	Überwachte iOS-Geräte Mit MDM aktivierte Samsung Knox-Geräte Windows 10 Education- und Windows 10 Enterprise-Geräte	Mit Rang	Beschränken der Apps, die auf einem Gerät ausgeführt werden können
Enterprise Management Agent	Konfigurieren, wie Geräte sich mit UEM verbinden, um App- oder Konfigurationsaktualisierungen zu erhalten.	iOS Android Windows	Mit Rang	Konfigurieren, wie Geräte BlackBerry UEM kontaktieren, um App- und Konfigurationsaktualisierungen zu erhalten
Gemeinsam genutztes iPad	Konfigurieren eines iPad-Geräts, damit es von mehreren Benutzern gemeinsam genutzt werden kann.	iOS	Mit Rang	Erstellen und Verwalten von Gruppen gemeinsam genutzter iPads
Konformität				
Konformität	Definieren der Gerätebedingungen, die in Ihrem Unternehmen nicht akzeptabel sind, und Konfigurieren entsprechender Erzwingungsaktionen.	Alle Geräte	Mit Rang	Durchsetzen von Kompatibilitätsregeln für Geräte
Konformität (BlackBerry Dynamics)	Dieses schreibgeschützte Profil zeigt die Konformitätseinstellungen an, die aus Good Control in eine lokale UEM-Umgebung importiert wurden.	Alle Geräte	Keine Angabe	Keine Angabe

Profilname	Beschreibung	Unterstützte Gerätetypen	Mit Rang oder ohne Rang	Weitere Informationen unter
Gerätedienstanforderungen	Konfigurieren der Softwareversionen, die auf Geräten installiert werden müssen.	Android	Mit Rang	Steuern, wie Softwareupdates auf Geräten installiert werden
E-Mail, Kalender und Kontakte				
E-Mail	Konfigurieren, wie Geräte eine Verbindung zum geschäftlichen E-Mail-Server herstellen und E-Mail-Nachrichten, Kalendereinträge und Terminplanerdaten synchronisieren.	Alle Geräte	Mit Rang	Erstellen von E-Mail-Profilen
IMAP/POP3-E-Mail	Konfigurieren, wie Geräte eine Verbindung mit einem IMAP- oder POP3-Mailserver herstellen, und Synchronisieren von E-Mail-Nachrichten.	Alle Geräte	Ohne Rang	Erstellen eines IMAP/POP3-E-Mail-Profils
Gatekeeping	Angeben der Microsoft Exchange-Server für das automatische Gatekeeping.	Alle Geräte	Mit Rang	Erstellen eines Gatekeeping-Profils
CalDAV	Angeben der Servereinstellungen, die Geräte verwenden können, um die Kalenderdaten zu synchronisieren.	iOS macOS	Ohne Rang	Einrichten von CardDAV- und CalDAV-Profilen
CardDAV	Angeben der Servereinstellungen, die Geräte verwenden können, um die Kontaktdaten zu synchronisieren.	iOS macOS	Ohne Rang	Einrichten von CardDAV- und CalDAV-Profilen
Netzwerke und Verbindungen				
Wi-Fi	Angeben, wie Geräte eine Verbindung mit einem geschäftlichen Wi-Fi-Netzwerk herstellen.	Alle Geräte	Ohne Rang	Einrichten von geschäftlichen WLAN-Netzwerken für Geräte
VPN	Konfigurieren, wie Geräte eine Verbindung mit einem geschäftlichen VPN herstellen.	Alle Geräte	Ohne Rang	Einrichten von geschäftlichen VPNs für Geräte

Profilname	Beschreibung	Unterstützte Gerätetypen	Mit Rang oder ohne Rang	Weitere Informationen unter
DNS	Angeben der DNS-Server, die Geräte für den Zugriff auf bestimmte Domänen verwenden.	iOS macOS	Mit Rang	Angeben von DNS-Servern für iOS- und macOS-Geräte
Proxy	Konfigurieren, wie Geräte einen Proxyserver für den Zugriff auf Webdienste im Internet oder in einem geschäftlichen Netzwerk verwenden.	iOS macOS Android	Mit Rang	Einrichten von Proxy-Profilen für Geräte
Enterprise-Konnektivität	Konfigurieren, wie Geräte über die Enterprise-Konnektivität eine Verbindung zu den Ressourcen Ihres Unternehmens herstellen können und ob Geräte BlackBerry Secure Connect Plus verwenden können.	iOS Android	Mit Rang	Verwenden von BlackBerry Secure Connect Plus für sichere Verbindungen mit geschäftlichen Ressourcen
BlackBerry Dynamics-Verbindungen	Konfigurieren der Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.	Alle Geräte	Mit Rang	Einrichten von Netzwerkverbindungen für BlackBerry Dynamics-Apps
BlackBerry 2FA	Aktivieren der Zwei-Faktor-Authentifizierung für Benutzer und Konfigurieren der Funktionen für die Vorauthentifizierung und Wiederherstellung.	iOS Android	Mit Rang	Erstellen eines BlackBerry 2FA-Profils
Netzwerknutzung	Konfigurieren, ob geschäftliche Apps auf iOS-Geräten das Mobilfunknetz oder Datenroaming verwenden dürfen.	iOS	Mit Rang	Steuern der Netzwerknutzung von Apps auf iOS-Geräten
Webinhaltsfilter	Begrenzen der Websites, die Benutzer auf überwachten iOS-Geräten anzeigen können.	Überwachte iOS-Geräte	Ohne Rang	Erstellen von Webinhaltsfilter-Profilen auf iOS-Geräten

Profilname	Beschreibung	Unterstützte Gerätetypen	Mit Rang oder ohne Rang	Weitere Informationen unter
SSO-Erweiterung	iOS-Geräten ermöglichen, sich bei Domänen und Webdiensten Ihres Unternehmensnetzwerks automatisch zu authentifizieren.	iOS	Ohne Rang	Aktivieren der automatische Authentifizierung für iOS-Geräte
Verwaltete Domänen	Konfigurieren von iOS-Geräten, damit Benutzer benachrichtigt werden, wenn sie E-Mails außerhalb von vertrauenswürdigen Domänen senden, und Einschränken der Apps, die aus internen Domänen heruntergeladene Dokumente öffnen können.	iOS	Ohne Rang	Angeben von E-Mail- und Webdomänen für iOS-Geräte
AirPrint	Fügen Sie Drucker zu AirPrint-Druckerlisten der Benutzer hinzu.	iOS	Ohne Rang	Erstellen eines AirPrint-Profils für iOS-Geräte
AirPlay	Fügen Sie Geräte zu AirPlay-Gerätelisten von Benutzern hinzu.	iOS	Ohne Rang	Erstellen eines AirPlay-Profils für iOS-Geräte
Zugriffspunktname	Angeben von APNs für Geräte, die für die Verbindung mit Betreibern verwendet werden sollen.	Android	Ohne Rang	Erstellen eines APN-Profils für Android-Geräte
Schutz				
Windows-Datenschutz	Konfigurieren der Windows-Datenschutzeinstellung in Windows 10.	Windows 10	Mit Rang	Einrichten von Windows-Unternehmensdatenschutz für Windows 10-Geräte
Microsoft Intune-App-Schutz	Konfigurieren, wie Daten in Office 365-Apps geschützt werden.	iOS Android	Ohne Rang	Verwalten von durch Microsoft Intune geschützten Apps
Standortdienst	Anfordern des Standorts von Geräten und Anzeigen der ungefähren Gerätestandorte auf einer Karte.	iOS Android Windows	Mit Rang	Verwenden von Standortdiensten auf Geräten

Profilname	Beschreibung	Unterstützte Gerätetypen	Mit Rang oder ohne Rang	Weitere Informationen unter
Nicht stören	Blockieren von BlackBerry Work-Benachrichtigungen während Ausschaltzeiten.	iOS Android	Mit Rang	Deaktivieren von Benachrichtigungen außerhalb der Arbeitszeiten von BlackBerry Work
Werkseitiger Rücksetzschutz	Steuern der werkseitigen Rücksetzschutzfunktion auf Android-Geräten.	Android	Mit Rang	Verwalten des werkseitigen Rücksetzschutzes für Android Enterprise- und Android Management-Geräte
CylancePROTECT	Konfigurieren der Sicherheitsfunktionen von CylancePROTECT Mobile for BlackBerry UEM.	iOS Android	Mit Rang	CylancePROTECT Mobile für BlackBerry UEM
Benutzerdefiniert				
Gerät	Angeben der Informationen, die auf den Geräten angezeigt werden.	iOS Android Windows	Mit Rang	Anzeigen von Organisationsinformationen auf Geräten
Startbildschirm-Layout	Konfigurieren des Layouts von Apps auf iOS-Geräten.	iOS	Mit Rang	Konfigurieren des Layouts von Apps auf iOS-Geräten
Benutzerdefinierte Payload	Angeben benutzerdefinierter Geräte-Konfigurationsinformationen mithilfe des Payload-Codes.	iOS	Ohne Rang	Verwalten von iOS-Funktionen mit benutzerdefinierten Payload-Profilen
Per-App-Benachrichtigung	Konfigurieren von Benachrichtigungseinstellungen für System-Apps und Apps, die Sie mit UEM verwalten.	Überwachte iOS-Geräte	Mit Rang	Verwalten Sie App-Benachrichtigungen auf überwachten iOS-Geräten
Zertifikate				
Zertifizierungsstell	Legen Sie ein Zertifizierungsstellenzertifikat fest, das von Geräten verwendet werden kann, um Vertrauen mit einem geschäftlichen Netzwerk oder einem Server aufzubauen.	Alle Geräte	Ohne Rang	Senden von Zertifizierungsstellenzertifikaten an Geräte und Apps

Profilname	Beschreibung	Unterstützte Gerätetypen	Mit Rang oder ohne Rang	Weitere Informationen unter
Freigegebenes Zertifikat	Legen Sie ein Client-Zertifikat fest, das Geräte für die Authentifizierung von Benutzern mit einem geschäftlichen Netzwerk oder Server verwenden können.	iOS macOS Android	Ohne Rang	Senden des gleichen Clientzertifikats an mehrere Geräte
Benutzeranmeldeir	Legen Sie die Zertifizierungsstellenverbindung fest, die Geräte verwenden, um ein Client-Zertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	iOS macOS Android	Ohne Rang	Senden von Clientzertifikaten an Geräte und Apps unter Verwendung von Profilen für Benutzeranmeldeinformationen
SCEP	Legen Sie den SCEP-Server fest, den Geräte verwenden, um ein Client-Zertifikat für die Authentifizierung mit einem geschäftlichen Netzwerk oder Server abzurufen.	Alle Geräte	Ohne Rang	Senden von Clientzertifikaten an Geräte und Apps mithilfe von SCEP
OCSP	Aktivieren von Geräten, um den Status von S/MIME-Zertifikaten zu überprüfen.	iOS Android	Mit Rang	Ermitteln des Status von S/MIME-Zertifikaten auf Geräten
CRL	Konfigurieren von UEM, um nach dem Status von S/MIME-Zertifikaten zu suchen.	iOS Android	Mit Rang	Ermitteln des Status von S/MIME-Zertifikaten auf Geräten
Profil mit Zertifikatzuordnun	Angeben, welche Kundenzertifikate Apps verwenden müssen.	Android	Mit Rang	Angeben des Zertifikats, das von einer App mit einem Zertifikatzuordnungsprofil verwendet wird

Verwalten von Profilen

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile**.
2. Klicken Sie auf den entsprechenden Profiltypen.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Kopieren eines Profils.	**a.** Klicken Sie auf den Namen des Profils, das Sie kopieren möchten. **b.** Klicken Sie auf . **c.** Geben Sie einen Namen und eine Beschreibung für das Profil ein. **d.** Konfigurieren Sie die entsprechenden Werte für das Profil. Weitere Informationen zu den einzelnen Profiltypen finden Sie unter BlackBerry UEM-Profile. **e.** Klicken Sie auf **Speichern**. **f.** Weisen Sie das Profil Benutzern und Gruppen zu.
Profil ändern.	**a.** Klicken Sie auf den Namen des Profils, das Sie ändern möchten. **b.** Klicken Sie auf . **c.** Nehmen Sie Änderungen am Profil vor. **d.** Klicken Sie auf **Speichern**.
Weisen Sie Profilen einen Rang zu.	**a.** Klicken Sie auf . **b.** Mit den Pfeiltasten können Sie die Profile in der Rangordnung nach oben oder unten verschieben. **c.** Klicken Sie auf **Speichern**.
Entfernen eines Profils aus Benutzerkonten.	**a.** Klicken Sie auf den Namen des Profils, das Sie entfernen möchten. **b.** Suchen Sie auf der Registerkarte **x Benutzern zugewiesen** nach den Benutzerkonten, aus denen Sie das Profil entfernen möchten, und wählen Sie diese aus. **c.** Klicken Sie auf .
Entfernen eines Profils aus Gruppen.	**a.** Klicken Sie auf den Namen des Profils, das Sie entfernen möchten. **b.** Suchen Sie auf der Registerkarte **x Gruppen zugewiesen** nach den Gruppen, aus denen Sie das Profil entfernen möchten, und wählen Sie diese aus. **c.** Klicken Sie auf .
Löschen eines Profils.	Sie können kein Standardprofil löschen. Wenn Sie ein benutzerdefiniertes Profil löschen, entfernt UEM es von den Benutzern und Geräten, zu denen eine Verknüpfung besteht. **a.** Klicken Sie auf das Profil, das Sie löschen möchten. **b.** Klicken Sie auf . **c.** Klicken Sie auf **Löschen**.

Verwenden von Variablen in Profilen, E-Mails und Benachrichtigungen

BlackBerry UEM unterstützt Standard- und benutzerdefinierte Variablen, die Sie in Profilen, Konformitätsbenachrichtigungen, Aktivierungs-E-Mails und Ereignisbenachrichtigungen verwenden können, um Konfigurationen und Nachrichten für einzelne Benutzer anzupassen. Standardvariablen stehen für standardmäßige Kontoattribute (z. B. Benutzername, E-Mail-Adresse) und andere vordefinierte Attribute (z. B. die zur Geräteaktivierung verwendete Serveradresse). Sie können benutzerdefinierte Variablen verwenden, um zusätzliche Attribute zu definieren.

Abgesehen von den Feldern „Name“ und „Beschreibung“ können Sie in jedem Textfeld eines Profils eine Variable verwenden. Beispielsweise können Sie „%UserName%@example.com“ in einem E-Mail-Profil im Feld „E-Mail-Adresse“ verwenden.

Sie können die Liste der Standardvariablen, die in der Verwaltungskonsole zur Verwendung verfügbar sind, unter **Einstellungen > Allgemeine Einstellungen > Standardvariablen anzeigen**.

Beachten Sie, dass IT-Richtlinien und BlackBerry Dynamics-App-Konfigurationen die Verwendung von Variablen nicht unterstützen.

Definieren von benutzerdefinierten Variablen

Sie können bis zu fünf benutzerdefinierte Textvariablen und bis zu fünf maskierte Textvariablen festlegen, um vertrauliche Informationen wie Kennwörter darzustellen. Wenn Sie eine benutzerdefinierte Variable festlegen, geben Sie eine Kennzeichnung für die Variable an (z. B. VPN-Kennwort). Wenn Sie ein Benutzerkonto erstellen oder aktualisieren, werden Kennzeichnungen als Feldnamen im Abschnitt „Benutzerdefinierte Variablen“ verwendet, und Sie können die entsprechenden Werte für diesen Benutzer angeben. Alle Benutzerkonten, einschließlich der Administratorkonten, unterstützen benutzerdefinierte Variablen. Sie können die benutzerdefinierten Variablen auf die gleiche Weise verwenden, wie Sie Standardvariablen verwenden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Benutzerdefinierte Variablen**.
2. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Variablen beim Hinzufügen oder Bearbeiten eines Benutzers anzeigen**.
3. Legen Sie eine Kennzeichnung für jede benutzerdefinierte Variable fest, die Sie verwenden möchten.
4. Klicken Sie auf **Speichern**.

Verwenden von E-Mail-Vorlagen, um Nachrichten an Benutzer zu senden

Sie können E-Mail-Vorlagen verwenden, um E-Mail-Nachrichten anzupassen und zu personalisieren, die BlackBerry UEM aus verschiedenen Gründen an Benutzer sendet, einschließlich Anweisungen zur Geräteaktivierung, Benachrichtigung von Benutzern über Konformitätsprobleme und Bereitstellung von Zugriffsschlüsseln für BlackBerry Dynamics-Apps.

Sie können E-Mail-Nachrichten personalisieren, indem Sie Variablen für Elemente wie den Namen, die E-Mail-Adresse oder das Aktivierungskennwort des Benutzers verwenden, und Sie können das Aussehen von Nachrichten mit verschiedenen Schriftarten, Farben und Bildern anpassen. Sie haben die Möglichkeit, mehrere Vorlagen zu erstellen, die für unterschiedliche Geräte- oder Aktivierungsarten verwendet werden können. Sie können die Standard-E-Mail-Vorlagen bearbeiten, oder Sie können neue Vorlagen erstellen.

Wenn Sie verschiedene Aufgaben in der Verwaltungskonsole ausführen (z. B. Hinzufügen eines Benutzers, Erstellen eines Konformitätsprofils usw.), können Sie die E-Mail-Vorlage auswählen, die UEM zum Senden einer Nachricht an Gerätebenutzer verwenden soll.

Sie können die verfügbaren Standardvorlagen in der Verwaltungskonsole unter „**Einstellungen > Allgemeine Einstellungen > Vorlagen**“ anzeigen.

Bearbeiten einer E-Mail-Vorlage

Wenn Sie eine Standard-E-Mail-Vorlage ändern möchten, wird empfohlen, eine Sicherungskopie des ursprünglichen Vorlagentextes zu speichern, falls Sie ihn später wiederherstellen möchten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Vorlagen**.
2. Klicken Sie auf die Vorlage, die Sie bearbeiten möchten.
3. Bearbeiten Sie die Felder **Name**, **Betreff** oder **Nachricht** wie erforderlich.
4. Klicken Sie auf **Speichern**.

Erstellen einer Vorlage für die Aktivierungs-E-Mail

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Vorlagen**.
2. Klicken Sie auf + > **Geräteaktivierung**.
3. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
4. Geben Sie im Feld **Betreff** die Betreffzeile der Aktivierungs-E-Mail ein.
5. Geben Sie den Nachrichtentext der Aktivierungs-E-Mail in das Feld **Nachrichten** ein.

   Verwenden Sie den HTML-Editor, um die Formatierung anzupassen, Bilder einzufügen (z. B. ein Firmenlogo) usw. Sie können Variablen einfügen, um Teile der E-Mail zu personalisieren. Siehe Verwenden von Variablen in Profilen, E-Mails und Benachrichtigungen.
6. Wenn Benutzer ihr Gerät mit einem QR Code anstelle eines Aktivierungskennworts aktivieren sollen, aktivieren Sie das Kontrollkästchen **QR-Code an die E-Mail-Nachricht für die iOS- und Android-Geräteaktivierung anhängen**.
7. Wählen Sie **Zwei Aktivierungs-E-Mails senden – die erste mit allen Anweisungen, die zweite mit dem Kennwort aus**, um das Aktivierungskennwort oder den QR Code getrennt von den Aktivierungsanweisungen

senden zu können, und geben Sie den Inhalt und die Optionen für die zweite Aktivierungs-E-Mail an. Wenn Sie entscheiden, nur eine Aktivierungs-E-Mail-Nachricht zu senden, überprüfen Sie, ob das Aktivierungskennwort, die Variable für das Aktivierungskennwort oder den QR Code in diese aufgenommen wurden.

8. Klicken Sie auf **Speichern**.

Weitere Informationen über Geräteaktivierung finden Sie unter Aktivieren von Geräten.

Erstellen einer Vorlage für Benachrichtigungen zur Vorschrifteneinhaltung

Wenn das Gerät eines Benutzers nicht die Anforderungen erfüllt, die Sie in einem zugewiesenen Konformitätsprofil konfiguriert haben, kann BlackBerry UEM auf Grundlage einer angegebenen Vorlage eine personalisierte E-Mail-Nachricht an den Benutzer senden. UEM umfasst eine Standard-E-Mail-Vorlage für Konformitätsverstöße, die bearbeitet, jedoch nicht gelöscht werden kann. Wenn einem Benutzerkonto keine andere Vorlage zugewiesen wird, verwendet UEM die Standardvorlage.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Vorlagen**.
2. Klicken Sie auf + > **Konformitätsverstoß**.
3. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
4. Geben Sie im Feld **Betreff** eine Betreffzeile für die Nachricht ein.
5. Geben Sie im Feld **Nachricht** den Nachrichtentext der E-Mail zur Vorschrifteneinhaltung ein.

   Verwenden Sie den HTML-Editor, um die Formatierung anzupassen, Bilder einzufügen (z. B. ein Firmenlogo) usw. Sie können Variablen einfügen, um Teile der E-Mail zu personalisieren. Siehe Verwenden von Variablen in Profilen, E-Mails und Benachrichtigungen.
6. Klicken Sie auf **Speichern**.

Weitere Informationen über Gerätekompatibilität finden Sie unter Durchsetzen von Kompatibilitätsregeln für Geräte.

Erstellen einer E-Mail-Vorlage für Ereignisbenachrichtigungen

Sie können eine E-Mail-Vorlage für Ereignisbenachrichtigungen erstellen, die BlackBerry UEM verwenden kann, um benutzerdefinierte Nachrichten an Administratoren zu senden , wenn bestimmte Ereignisse in der UEM-Umgebung Ihres Unternehmens auftreten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Vorlagen**.
2. Klicken Sie auf + > **Ereignisbenachrichtigung**.
3. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
4. Geben Sie im Feld **Betreff** eine Betreffzeile für die Nachricht ein. Wenn Sie den Ereignistyp an die Betreffzeile anhängen möchten, aktivieren Sie das Kontrollkästchen **Ereignistyp an E-Mail-Betreff anhängen**.
5. Geben Sie den Nachrichtentext der Ereignisbenachrichtigungs-E-Mail in das Feld **Nachricht** ein.

   Verwenden Sie den HTML-Editor, um die Formatierung anzupassen, Bilder einzufügen (z. B. ein Firmenlogo) usw. Sie können Variablen einfügen, um Teile der E-Mail zu personalisieren. Siehe Verwenden von Variablen in Profilen, E-Mails und Benachrichtigungen.
6. Klicken Sie auf **Speichern**.

Weitere Informationen über Ereignisbenachrichtigungen finden Sie unter Erstellen von Ereignisbenachrichtigungen.

Vorgeschlagener Text für Vorlagen

Der vorgeschlagene Text unten wird in E-Mail-Standardvorlagen verwendet. Wenn Sie die E-Mail-Standardvorlagen bearbeiten und später den Standardtext verwenden möchten, können Sie ihn hier kopieren und dann einfügen.

Name	Vorgeschlagener Text
Aktivierungscode für Android-Arbeitsprofil	**Betreff: Ein Aktivierungscode für ein Android-Arbeitsprofil wurde für Sie erstellt** %UserDisplayName%, Zum Aktivieren eines Android-Geräts nur mit einem Arbeitsprofil hat Ihr Administrator einen Android-Aktivierungscode für Sie erstellt. Ihr BlackBerry UEM-Aktivierungskennwort erhalten Sie in einer separaten E-Mail. Ihr Aktivierungscode für das Android-Arbeitsprofil lautet: %GoogleActivationCode % Ihr Aktivierungscode für das Android-Arbeitsprofil läuft am %ActivationPasswordExpiry % ab. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator.
Anmeldeinformatione für standardmäßige verwaltete Google-Konten	**Betreff: Ein Google-Konto wurde für Sie erstellt** %UserDisplayName%, Für die Aktivierung des Arbeitsprofils auf Ihrem Gerät hat Ihr Administrator ein Google-Konto für Sie erstellt. Sie benötigen für die Aktivierung des Arbeitsprofils das Kennwort für Ihr Google-Konto. Das hier angezeigte Kennwort für das Google-Konto ist nicht das Kennwort, das Sie verwenden, wenn Sie Ihr Gerät in BlackBerry UEM aktivieren. Sie erhalten Ihr BlackBerry UEM-Aktivierungskennwort in einer separaten E-Mail. Alternativ können Sie Ihr BlackBerry UEM-Aktivierungskennwort in BlackBerry UEM Self-Service einrichten. Für die Aktivierung des Arbeitsprofils benötigen Sie folgende Informationen: • Ihre geschäftliche E-Mail-Adresse: %UserEmailAddress% • Ihr Google-Kontokennwort: %Password% Sie können Ihr Google-Konto unter https://myaccount.google.com verwalten. Wenn Sie das Kennwort für Ihr Google-Konto ändern, ist das Kennwort in dieser E-Mail nicht mehr gültig. Sie müssen dann stattdessen das neue Kennwort verwenden. Bitte bewahren Sie diese Informationen für Ihre Unterlagen auf. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator.

Name	Vorgeschlagener Text
Apple DEP-Aktivierungs-E-Mail Erste E-Mail	**Betreff: Aktivierung Ihres Geräts in BlackBerry UEM** %UserDisplayName%, Ihr Administrator hat Ihr iOS-Gerät für BlackBerry UEM aktiviert. Um Ihr Gerät zu aktivieren, benötigen Sie die folgenden Informationen: • Ihre geschäftliche E-Mail-Adresse: %UserEmailAddress% • Ihr Geräteaktivierungskennwort: Ihr Aktivierungskennwort wird in einer separaten E-Mail zugestellt. Verwalten Sie Ihr Gerät mit BlackBerry UEM Self-Service unter %UserSelfServicePortalURL%. Verwenden Sie zum Anmelden den folgenden Benutzernamen: BlackBerry UEM Self-Service Benutzername: %UserName% Ihr BlackBerry UEM Self-Service-Kennwort wurde Ihnen möglicherweise bereits in einer separaten E-Mail zugesendet. Wenn Sie es nicht erhalten haben, wenden Sie sich an Ihren Administrator. Bitte bewahren Sie diese Informationen für Ihre Unterlagen auf. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator.
Apple DEP-Aktivierungs-E-Mail Zweite E-Mail	**Betreff: Kennwort zur Aktivierung Ihres Geräts in BlackBerry UEM** %UserDisplayName%, Ihr Administrator hat Ihr Mobilgerät für BlackBerry UEM aktiviert. Um Ihr Gerät zu aktivieren, benötigen Sie die folgenden Informationen: Ihr Geräteaktivierungskennwort: %ActivationPassword% Ihr Kennwort läuft am %ActivationPasswordExpiry% ab. Folgen Sie den Anweisungen in der E-Mail mit dem Betreff „Aktivierung Ihres Geräts in BlackBerry UEM“, um Ihr iOS-Gerät in BlackBerry UEM zu aktivieren. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator. Willkommen bei BlackBerry UEM

Name	Vorgeschlagener Text
Zugriffsschlüssel-E-Mail für BlackBerry Dynamics	**Betreff: Für Sie wurde ein Zugriffsschlüssel für eine BlackBerry Dynamics-App erstellt** %UserDisplayName%, Ihr Administrator hat einen Zugriffsschlüssel für eine BlackBerry Dynamics-App erstellt. Diese E-Mail enthält den Zugriffsschlüssel und Anweisungen zur Einrichtung der App. Wenn Ihnen Berechtigungen für mehrere Apps erteilt wurden, erhalten Sie mehrere E-Mails. Jede E-Mail enthält einen Zugriffsschlüssel zur Einrichtung einer App. Sie können jeden Schlüssel zur Einrichtung jeder beliebigen App verwenden, aber jeder Zugriffsschlüssel kann nur einmal verwendet werden. Stellen Sie zunächst sicher, dass Sie über Mobilfunk- oder Wi-Fi-Empfang verfügen. **1.** Öffnen Sie die BlackBerry Dynamics-App. **2.** Geben Sie nach Aufforderung folgende Informationen ein. • E-Mail-Adresse: %UserEmailAddress% • Zugriffsschlüssel: %AccessKeys% Ihr Zugriffsschlüssel läuft am %AccessKeyExpiry% ab. **3.** Möglicherweise werden Sie aufgefordert, ein Kennwort zu erstellen. Dieses Kennwort müssen Sie eingeben, wenn Sie die App öffnen. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator.

Name	Vorgeschlagener Text
Standardmäßige Aktivierungs-E-Mail Erste E-Mail	**Betreff: Aktivierung Ihres Geräts in BlackBerry UEM** %UserDisplayName%, Ihr Administrator hat Ihr Mobilgerät für BlackBerry UEM aktiviert. Um Ihr Gerät zu aktivieren, benötigen Sie einige oder alle der folgenden Informationen: • Ihre geschäftliche E-Mail-Adresse: %UserEmailAddress% • Servername: %ActivationURL% • Aktivierungsbenutzername: %ActivationUserName% • Ihr Geräteaktivierungskennwort: Ihr Aktivierungskennwort wird in einer separaten E-Mail zugestellt. Für Android-Geräte: Wenn Sie ein Android-Gerät verwenden, müssen Sie den BlackBerry UEM Client aus Google Play installieren. Für iOS-Geräte: Wenn Sie ein iOS-Gerät verwenden, müssen Sie den BlackBerry UEM Client aus dem App Store installieren. Öffnen Sie bei iOS-Geräten Safari, und navigieren Sie zu „workspace://apps“, um Apps zu installieren, die Ihr Administrator Ihnen zugewiesen hat. Falls verfügbar, können Sie auch auf Work Apps auf Ihrem Gerät tippen. Für macOS-Geräte: Wenn Sie ein macOS-Gerät verwenden, müssen Sie Ihr Gerät mit BlackBerry UEM Self-Service aktivieren. Für Geräte mit Windows 10 oder höher: Für die Aktivierung Ihres Geräts benötigen Sie die folgenden Informationen: • Servername: %ClientlessActivationURL% • URL des Zertifikatservers: %RsaRootCaCertUrl% • Sie müssen das RSA-Zertifikat installieren. Geben Sie die URL des Zertifikatservers in die Adresszeile des Browsers auf Ihrem Gerät ein. Befolgen Sie die Anweisungen, und installieren Sie das Zertifikat im Ordner „Vertrauenswürdige Stammzertifizierungsstellen“. • Navigieren Sie auf Ihrem Gerät zu „**Einstellungen > Konten > Auf Arbeits- oder Schulkonto zugreifen**“, und tippen Sie auf „Nur in Geräteverwaltung registrieren“. Verwaltung Ihrer Geräte Verwalten Sie Ihr Gerät mit BlackBerry UEM Self-Service unter %UserSelfServicePortalURL%. Verwenden Sie zum Anmelden den folgenden Benutzernamen: BlackBerry UEM Self-Service Benutzername: %UserName% Ihr BlackBerry UEM Self-Service-Kennwort wurde Ihnen möglicherweise bereits in einer separaten E-Mail zugesendet. Willkommen bei BlackBerry UEM

Name	Vorgeschlagener Text
Standardmäßige Aktivierungs-E-Mail Zweite E-Mail	**Betreff: Kennwort zur Aktivierung Ihres Geräts in BlackBerry UEM** %UserDisplayName%, Ihr Administrator hat Ihr Mobilgerät für BlackBerry UEM aktiviert. Um Ihr Gerät zu aktivieren, benötigen Sie die folgenden Informationen: • Ihr Geräteaktivierungskennwort: %ActivationPassword% • Ihr Kennwort läuft am %ActivationPasswordExpiry% ab. Folgen Sie den Anweisungen in der E-Mail mit dem Betreff „Aktivierung Ihres Geräts in BlackBerry UEM“, um Ihr iOS-, Android- oder Windows-Gerät in BlackBerry UEM zu aktivieren. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator. Willkommen bei BlackBerry UEM
Standardmäßige Android Management-Aktivierungs-E-Mail	**Betreff: Aktivierung Ihres Geräts in BlackBerry UEM** %UserDisplayName%, Ihr Administrator hat Android Management auf Ihrem Gerät aktiviert, damit ein geschäftliches Profil erstellt werden kann. Um das geschäftliche Profil zu erstellen, können Sie auf Ihrem Gerät auf den folgenden Link klicken: %ActivationAndroidManagementURL%. Sie können auch den QR-Code auf Ihrem Gerät scannen. Navigieren Sie zu **Einstellungen > Google-Dienste > Einrichtung und Wiederherstellung > Geschäftliches Profil einrichten**, und scannen Sie dann den folgenden QR-Code. Der Aktivierungslink und der QR-Code laufen am %ActivationPasswordExpiry% ab. %ActivationAndroidManagementQRCode% Bitte bewahren Sie diese Informationen für Ihre Unterlagen auf. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator.
Standard-E-Mail für Konformitätsverstöße	**Betreff: Benachrichtigung über ein nicht kompatibles Gerät** Ihr Gerät ist mit den Richtlinien Ihres Unternehmens nicht kompatibel. Wenn dieser Zustand bestehen bleibt, kann der Administrator den Zugriff auf die Unternehmensdaten von Ihrem Gerät aus einschränken, Unternehmensdaten bzw. alle Inhalte und Einstellungen auf Ihrem Gerät löschen.

Name	Vorgeschlagener Text
Standardmäßige Aktivierungs-E-Mail für „Nur geschäftlicher Bereich (Android Enterprise) Erste E-Mail	**Betreff: Aktivierung Ihres Geräts in BlackBerry UEM** %UserDisplayName%, Ihr Administrator hat Ihr Android-Gerät (9.0 und höher) für BlackBerry UEM aktiviert. Um Ihr Gerät zu aktivieren, benötigen Sie die folgenden Informationen: • Aktivierungsbenutzername: %ActivationUserName% • Ihr Geräteaktivierungskennwort: Ihr Aktivierungskennwort wird in einer separaten E-Mail zugestellt. Gehen Sie wie folgt vor, um Ihr Gerät zu aktivieren: **1.** Wenn Ihnen der Willkommen-Bildschirm der Geräteeinrichtung nicht angezeigt wird, setzen Sie das Gerät auf die werksseitigen Standardeinstellungen zurück. **2.** Geben Sie während der Geräteeinrichtung im Bildschirm „Ihr Konto hinzufügen“ die Anmeldedaten für Ihr Google-Konto ein. Warten Sie, während das Gerät wichtige System-Apps aktualisiert und den UEM Client herunterlädt. **3.** Folgen Sie im BlackBerry UEM Client den Anweisungen auf dem Bildschirm, um Ihr Gerät zu aktivieren. Verwalten Sie Ihr Gerät mit BlackBerry UEM Self-Service unter %UserSelfServicePortalURL%. Verwenden Sie zum Anmelden den folgenden Benutzernamen: BlackBerry UEM Self-Service Benutzername: %UserName% Ihr BlackBerry UEM Self-Service-Kennwort wurde Ihnen möglicherweise bereits in einer separaten E-Mail zugesendet. Wenn Sie es nicht erhalten haben, wenden Sie sich an Ihren Administrator. Bitte bewahren Sie diese Informationen für Ihre Unterlagen auf. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator. Willkommen bei BlackBerry UEM
Standardmäßige E-Mail-Vorlage für die Aktivierung von „Nur geschäftlicher Bereich“ (Android-Arbeitsprofile) Zweite E-Mail	**Betreff: Kennwort zur Aktivierung Ihres Geräts in BlackBerry UEM** %UserDisplayName%, Ihr Administrator hat Ihr Android-Gerät für BlackBerry UEM aktiviert. Um Ihr Gerät zu aktivieren, benötigen Sie die folgenden Informationen: • Ihr Geräteaktivierungskennwort: %ActivationPassword% • Ihr Kennwort läuft am %ActivationPasswordExpiry% ab. Folgen Sie den Anweisungen in der E-Mail mit dem Betreff „Aktivierung Ihres Geräts in BlackBerry UEM“, um Ihr Gerät in BlackBerry UEM zu aktivieren. Wenn Sie Fragen haben, wenden Sie sich an Ihren Administrator. Willkommen bei BlackBerry UEM !
E-Mail zur Ereignisbenachrichtig für BlackBerry UEM	**Betreff: BlackBerry UEM-Ereignisbenachrichtigung** Folgendes Ereignis ist eingetreten: %AllEventVariables%

Name	Vorgeschlagener Text
Geräteaktivierte Benachrichtigung	**Betreff: Gerät in BlackBerry UEM aktiviert** %UserDisplayName%, Ihr Gerät wurde in BlackBerry UEM aktiviert. Geräteinformationen Modell: %DeviceModel% Seriennummer: %SerialNumber % IMEI: %DeviceIMEI% Wenn Sie dieses Gerät nicht aktiviert haben, wenden Sie sich an Ihren Administrator. **Betreff: BlackBerry Dynamics-Gerät in BlackBerry UEM aktiviert** %UserDisplayName%, Ihr BlackBerry Dynamics-Gerät wurde in BlackBerry UEM aktiviert. Wenn Sie dieses Gerät nicht aktiviert haben, wenden Sie sich an Ihren Administrator.
Benachrichtigung für Self-Service-Anmeldung	**Betreff: Benachrichtigung für Self-Service-Anmeldung** %UserDisplayName%, Sie haben sich bei BlackBerry UEM Self-Service angemeldet. IP-Adressbereich: %IPAddress% Zeit: %Timestamp% Wenn Sie sich nicht angemeldet haben, wenden Sie sich an Ihren Administrator.

Verwalten von Geräten mit IT-Richtlinien

Sie können IT-Richtlinien zum Verwalten der Sicherheit und des Verhaltens von Geräten in der BlackBerry UEM-Umgebung Ihres Unternehmens verwenden. Eine IT-Richtlinie ist ein Satz von Regeln, mit denen Sie Gerätefunktionen und -funktionalität steuern können. Sie können beispielsweise IT-Richtlinienregeln verwenden, um Kennwortanforderungen durchzusetzen, die Verwendung bestimmter Gerätefunktionen (z. B. der Kamera) zu verhindern und die Verfügbarkeit bestimmter Apps zu steuern.

Sie können Regeln für alle Gerätearten in derselben IT-Richtlinie konfigurieren. Das Betriebssystem des Geräts bestimmt die Funktionen, die mithilfe von IT-Richtlinienregeln gesteuert werden können. Die Geräteaktivierungsart legt fest, welche Regeln für ein bestimmtes Gerät gelten und ob Sie Regeln verwenden können, um das gesamte Gerät oder nur den geschäftlichen Bereich zu steuern. Geräte ignorieren nicht zutreffende IT-Richtlinienregeln.

Laden Sie die Tabelle der IT-Richtlinienregeln herunter, um eine umfassende Referenz aller verfügbaren IT-Richtlinienregeln für jeden von UEM unterstützten Gerätetyp zu erhalten.

UEM enthält eine Standard-IT-Richtlinie mit vorkonfigurierten Regeln für jede Geräteart. Sie können die Standard-IT-Richtlinie an die Anforderungen Ihres Unternehmens anpassen. Wenn einem Benutzerkonto, einer Benutzergruppe, der ein Benutzer angehört, oder einer Gerätegruppe, dem die Geräte eines Benutzers angehören, keine IT-Richtlinie zugewiesen ist, sendet UEM die Standard-IT-Richtlinie an die Geräte des Benutzers. 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.

UEM weist einem Gerät nur eine IT-Richtlinie zu und verwendet vordefinierte Regeln, um zu bestimmen, welche IT-Richtlinie zugewiesen werden soll. Eine IT-Richtlinie, die einem Benutzer direkt zugewiesen wurde, hat Vorrang vor einer IT-Richtlinie, die über die Mitgliedschaft in einer Benutzergruppe zugewiesen wird. Wenn ein Benutzer Mitglied mehrerer Benutzergruppen mit unterschiedlichen IT-Richtlinien ist, wird anhand einer Rangfolge festgelegt, welche IT-Richtlinie zugewiesen wird. Wenn das Gerät eines Benutzers zu einer Gerätegruppe gehört, hat die der Gerätegruppe zugewiesene IT-Richtlinie Vorrang vor einer IT-Richtlinie, die dem Benutzer direkt zugewiesen ist. Wenn das Gerät Mitglied mehrerer Gerätegruppen mit unterschiedlichen IT-Richtlinien ist, wird anhand einer Rangfolge festgelegt, welche IT-Richtlinie zugewiesen wird.

IT-Richtlinien verwalten

Sie können die Standard-IT-Richtlinie ändern oder benutzerdefinierte IT-Richtlinien erstellen und zuweisen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Richtlinie > IT-Richtlinien**.
2. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Erstellen Sie eine IT-Richtlinie.	**a.** Klicken Sie auf +. **b.** Geben Sie einen Namen und eine Beschreibung für die IT-Richtlinie ein. **c.** Klicken Sie für jeden Gerätetyp auf die Registerkarte, und konfigurieren Sie die entsprechenden Werte für die IT-Richtlinienregeln. Weitere Informationen zu IT-Richtlinienregeln finden Sie in der Tabelle der IT-Richtlinienregeln. **d.** Klicken Sie auf **Speichern**. **e.** Weisen Sie die IT-Richtlinie Benutzern und Gruppen zu.

Aufgabe	Schritte
Kopieren einer IT-Richtlinie.	**a.** Klicken Sie auf den Namen der IT-Richtlinie, die Sie kopieren möchten. **b.** Klicken Sie auf . **c.** Geben Sie einen Namen und eine Beschreibung für die IT-Richtlinie ein. **d.** Klicken Sie für jeden Gerätetyp auf die Registerkarte, und konfigurieren Sie die entsprechenden Werte für die IT-Richtlinienregeln. Weitere Informationen zu IT-Richtlinienregeln finden Sie in der Tabelle der IT-Richtlinienregeln. **e.** Klicken Sie auf **Speichern**. **f.** Weisen Sie die IT-Richtlinie Benutzern und Gruppen zu.
Ändern einer IT-Richtlinie.	**a.** Klicken Sie auf den Namen der IT-Richtlinie, die Sie ändern möchten. **b.** Klicken Sie auf . **c.** Nehmen Sie die gewünschten Änderungen für jeden Gerätetyp auf der entsprechenden Registerkarte vor. **d.** Klicken Sie auf **Speichern**.
Weisen Sie IT-Richtlinien einen Rang zu.	**a.** Klicken Sie auf . **b.** Mit den Pfeiltasten können Sie die IT-Richtlinien in der Rangordnung nach oben oder unten verschieben. **c.** Klicken Sie auf **Speichern**.
Entfernen einer IT-Richtlinie von Benutzerkonten.	**a.** Klicken Sie auf den Namen der IT-Richtlinie, die Sie entfernen möchten. **b.** Suchen Sie auf der Registerkarte **x Benutzern zugewiesen** nach den Benutzerkonten, aus denen Sie die IT-Richtlinie entfernen möchten, und wählen Sie diese aus. **c.** Klicken Sie auf .
Entfernen einer IT-Richtlinie von Gruppen	**a.** Klicken Sie auf den Namen der IT-Richtlinie, die Sie entfernen möchten. **b.** Suchen Sie auf der Registerkarte **x Gruppen zugewiesen** nach den Gruppen, aus denen Sie die IT-Richtlinie entfernen möchten, und wählen Sie diese aus. **c.** Klicken Sie auf .
Löschen einer IT-Richtlinie.	Sie können die Standard-IT-Richtlinie nicht löschen. Wenn Sie eine benutzerdefinierte IT-Richtlinie löschen, entfernt UEM die IT-Richtlinie aus den Benutzern und deren verknüpften Geräten. **a.** Klicken Sie auf die IT-Richtlinie, die Sie löschen möchten. **b.** Klicken Sie auf . **c.** Klicken Sie auf **Löschen**.
Exportieren von IT-Richtlinien in eine XML-Datei.	**a.** Wählen Sie die IT-Richtlinien, die Sie exportieren möchten. **b.** Klicken Sie auf .

Manuelles Importieren von Updates für IT-Richtlinien und Gerätemetadaten

BlackBerry sendet regelmäßig Updates für IT-Richtlinien und Gerätemetadaten an BlackBerry UEM. Wenn beispielsweise ein Anbieter ein neues Gerätemodell herausgibt, kann BlackBerry aktualisierte Gerätemetadaten an UEM senden, sodass Aktivierungs- und Konformitätsprofile das neue Gerätemodell enthalten. Wenn ein Anbieter ein Betriebssystemupdate veröffentlicht, wird möglicherweise ein neues IT-Richtlinienpaket an UEM gesendet, damit Sie neue Betriebssystemfunktionen verwalten können.

Standardmäßig empfängt und installiert UEM diese Updates automatisch. Wenn die Sicherheitsrichtlinie Ihres Unternehmens automatische Updates nicht zulässt und Sie eine lokale UEM-Umgebung haben, können Sie die automatischen Updates deaktivieren und Updates manuell importieren. Aktualisierungsdateien sind kumulativ. Wenn Sie ein Update verpassen, werden mit dem nächsten Update alle zuvor aktualisierten IT-Richtlinienregeln oder Gerätemetadaten installiert. Sie können Ereignisbenachrichtigungen einrichten, um Administratoren darüber zu informieren, wenn Updates für IT-Richtlinien und Gerätemetadaten installiert sind.

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

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Infrastruktur > Konfigurationsdaten importieren**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Um die automatischen Updates für IT-Richtlinienpakete zu deaktivieren, deaktivieren Sie das Kontrollkästchen **IT-Richtlinienpaketdate automatisch aktualisieren**.
   - Um die automatischen Updates für Gerätemetadaten zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Gerätemetadaten automatisch aktualisieren**.
3. Klicken Sie auf die entsprechende Schaltfläche **Durchsuchen**, um zu der Datendatei zu navigieren, die Sie importieren möchten, und sie auszuwählen. Klicken Sie auf **Öffnen**.

Erstellen von Geräte-Supportmeldungen für deaktivierte Funktionen auf Android-Geräten

Für Geräte mit Android 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.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Benutzerdefinierte Geräte-Supportmeldungen**.
2. Wählen Sie in der Dropdown-Liste **Gerätesprache** die Sprache aus, in der die Benachrichtigung angezeigt werden soll.
3. Geben Sie im Feld **Hinweis zu deaktivierten Funktionen** den Text ein, der auf Geräten angezeigt werden soll, wenn eine Funktion deaktiviert ist.
4. Optional können Sie im Feld **Administrator-Supportmeldung** einen Hinweis eingeben, der auf dem Einstellungsbildschirm des Geräteadministrators angezeigt wird.
5. Wenn Sie eine Nachricht in mehr als einer Sprache erstellen möchten, klicken Sie auf **Eine weitere Sprache hinzufügen**, und wiederholen Sie die vorherigen Schritte.
6. Wenn Sie Nachrichten in mehr als einer Sprache hinzugefügt haben, wählen Sie das Optionsfeld **Standardsprache** neben der Sprache aus, die auf Geräten verwendet werden soll, die keine der angegebenen Sprachen verwenden.
7. 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 Konformitätsprofil legt die Bedingungen fest, die ein Gerät nicht konform machen würden, die Benachrichtigungen, die ein Benutzer erhält, wenn ein Gerät nicht konform ist, und die Maßnahmen, die BlackBerry UEM ergreift, wenn ein Konformitätsproblem nicht gelöst wird (z. B. Beschränkung des Zugriffs eines Benutzers auf die Ressourcen des Unternehmens, Löschen von geschäftlichen Daten vom Gerät oder Löschen aller Daten vom Gerät).

UEM enthält ein Standard-Konformitätsprofil. Das Standard-Konformitätsprofil setzt keine Konformitätsbedingungen durch. Um Konformitätsregeln durchzusetzen, können Sie die Einstellungen des Standard-Konformitätsprofils ändern oder benutzerdefinierte Konformitätsprofile erstellen und zuweisen. Benutzerkonten, denen kein benutzerdefiniertes Konformitätsprofil zugewiesen wird, wird das Standard-Konformitätsprofil zugewiesen.

Bei Samsung Knox-Geräten können Sie eine Liste der gesperrten Apps zu einem Konformitätsprofil hinzufügen, aber UEM setzt die Konformitätsregeln nicht 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 Dynamics-Kompatibilitätsprofile werden von Good Control importiert, wenn Sie Good Control mit UEM synchronisieren. Sie können BlackBerry Dynamics-Konformitätsprofile nicht bearbeiten, aber sie können als Referenz zum Erstellen neuer Konformitätsprofile in UEM verwendet werden. Benutzer, die einem Kompatibilitätsprofil in Good Control zugewiesen wurden, bleiben nach der Synchronisierung mit UEM weiterhin demselben Profil zugewiesen. Wenn ein Benutzer einem BlackBerry Dynamics-Konformitätsprofil zugewiesen wird, hat das BlackBerry Dynamics-Konformitätsprofil Vorrang vor allen BlackBerry Dynamics-Regeln in den UEM-Konformitätsprofilen, die einem Benutzer ebenfalls zugewiesen werden können.

Erstellen eines Kompatibilitätsprofils

Bevor Sie beginnen:

- Wenn Sie Regeln zum Sperren oder Zulassen bestimmter Apps definieren wollen, fügen Sie die jeweiligen Apps der Liste der gesperrten Apps hinzu. Weitere Informationen finden Sie unter Hinzufügen einer App zur Liste der gesperrten Apps. Dies gilt nicht für integrierte Apps für überwachte iOS-Geräte. 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 und iPadOS: Einstellungen für Konformitätsprofil.
- 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 zur Konformität.

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 der Verwaltungskonsole auf **Richtlinien und Profile > Konformität > Konformität**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.

4. Wählen Sie in der Dropdown-Liste **Gesendete E-Mail bei Erkennung einer Verletzung** eine E-Mail-Vorlage aus.
5. Wählen Sie in der Drop-down-Liste **Erzwingungsintervall** die Häufigkeit der Konformitätsprüfungen für BlackBerry Dynamics-Apps aus. Sie können das Erzwingungsintervall für Nicht-BlackBerry Dynamics-Konformitätsprüfungen nicht konfigurieren. Diese werden in regelmäßigen Abständen durchgeführt.
6. Erweitern Sie **Gesendete Gerätebenachrichtigung bei Erkennung einer Verletzung**, und bearbeiten Sie die Nachricht nach Bedarf. Sie können Variablen in der Nachricht verwenden, um bestimmte Benutzer-, Geräte- und Konformitätsinformationen hinzuzufügen. Siehe Verwenden von Variablen in Profilen, E-Mails und Benachrichtigungen.
7. 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 an folgender Stelle:
   - Allgemein: Einstellungen für Kompatibilitätsprofil
   - iOS und iPadOS: Einstellungen für Konformitätsprofil
   - macOS: Kompatibilitätsprofil-Einstellungen
   - Android: Kompatibilitätsprofil-Einstellungen
   - Windows: Kompatibilitätsprofil-Einstellungen
8. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.

Allgemein: Einstellungen für Kompatibilitätsprofil

Für jede ausgewählte Konformitätsregel wählen Sie auf den Geräte-Registerkarten die Aktion, die BlackBerry UEM durchführen soll, wenn das Gerät eines Benutzers eine Richtlinie verletzt:

Einstellung für Konformitätsprofil	Beschreibung
Verhalten für Eingabeaufforderung	Diese Einstellung gibt an, ob UEM den Benutzer auffordert, ein Konformitätsproblem zu korrigieren, und dem Benutzer Zeit gibt, das Problem zu beheben, bevor er Maßnahmen ergreift, oder ob UEM sofort Maßnahmen ergreift.
Aufforderungsmethode	Diese Einstellung legt fest, ob der Benutzer von UEM aufgefordert wird, ein Konformitätsproblem durch Senden einer Gerätebenachrichtigung oder einer E-Mail-Nachricht und einer Gerätebenachrichtigung zu beheben. BlackBerry Dynamics-Apps bieten unabhängig von dieser Einstellung nur Gerätebenachrichtigungen. Gerätebenachrichtigungen werden auf Windows 10-Geräten nicht unterstützt. Diese Einstellung gilt nur, wenn das „Verhalten für Eingabeaufforderung“ auf „Kompatibilitätsprüfung fordern“ festgelegt ist.
Anzahl der Aufforderungen	Diese Einstellung gibt an, wie oft der Benutzer aufgefordert wird, ein Kompatibilitätsproblem zu beheben. Diese Einstellung gilt nur, wenn das „Verhalten für Eingabeaufforderung“ auf „Kompatibilitätsprüfung fordern“ festgelegt ist.

Einstellung für Konformitätsprofil	Beschreibung
Aufforderungsintervall	Diese Einstellung gibt die Zeitspanne zwischen den Aufforderungen in Minuten, Stunden oder Tagen an. Diese Einstellung gilt nur, wenn das „Verhalten für Eingabeaufforderung“ auf „Kompatibilitätsprüfung fordern“ festgelegt ist.
Erzwingungsaktion für Gerät	Diese Einstellung gibt die Aktion an, die UEM auf Geräten durchführt, die nicht kompatibel sind. Die verfügbaren Optionen können je nach Betriebssystem und Art der Konformitätsregel variieren: • Überwachen und protokollieren: UEM identifiziert den Konformitätsverstoß, ergreift jedoch keine Erzwingungsmaßnahme auf dem Gerät. • Nicht vertrauen: Der Benutzer kann nicht auf geschäftliche Ressourcen und Apps auf dem Gerät zugreifen. Daten und Apps werden nicht gelöscht. Auf iPadOS- und 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. • Nur geschäftliche Daten löschen • Alle Daten löschen • Von Server entfernen Diese Einstellung gilt nicht für Geräte mit Privatsphäre des Benutzers-Aktivierung. 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 UEM die gleiche Aktion wie bei „Nur geschäftliche Daten löschen“ aus. Auf Samsung Knox Workspace-Geräten, die nur über einen geschäftlichen Bereich verfügen, werden bei Auswahl der Option „Nur geschäftliche Daten löschen“, „Alle Daten löschen“ oder „Von Server entfernen“ alle Daten vom Gerät gelöscht. Bei iOS- und iPadOS-Geräten unter Aufsicht gelten keine Erzwingungsaktionen für die Regel „Eine gesperrte App wurde installiert“. Es wird automatisch verhindert, dass Benutzer gesperrte Apps installieren.
Erzwingungsaktion für BlackBerry Dynamics-Apps	Diese Einstellung gibt an, was mit BlackBerry Dynamics-Apps geschieht, wenn ein Gerät nicht kompatibel ist. • Ausführen von BlackBerry Dynamics-Apps nicht zulassen • BlackBerry Dynamics-Appdaten löschen • Überwachen und protokollieren: UEM identifiziert den Konformitätsverstoß, ergreift jedoch keine Erzwingungsmaßnahme.

iOS und iPadOS: Einstellungen für Konformitätsprofil

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der Erzwingungsaktionen, die BlackBerry UEM ausführen kann, wenn ein Gerät eine Konformitätsregel verletzt.

Einstellung für Konformitätsprofil	Beschreibung
Betriebssystem mit Jailbreak	Durch diese Einstellung wird eine Konformitätsregel erstellt, um zu gewährleisten, dass 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 Geräte durchführen, auf denen ein Jailbreak aufgetreten ist, 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. Diese Einstellung gilt nicht für Geräte mit der Aktivierungsart Privatsphäre des Benutzers.
Eine erforderliche App wurde nicht installiert.	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu gewährleisten, dass auf Geräten die erforderlichen Apps installiert sind.
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten keine gesperrten Betriebssystemversionen installiert werden. 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 zu sperren. 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 UEM sind. Sie geben die Anzahl der Tage an, die ein Gerät ohne Kontakt zu UEM sein kann, bevor davon ausgegangen wird, dass es nicht mehr kompatibel ist.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliothekversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.

Einstellung für Konformitätsprofil	Beschreibung
Überprüfung der BlackBerry Dynamics-Verbindung	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu überwachen, ob BlackBerry Dynamics-Apps länger als eine angegebene Zeitspanne ohne Kontakt zu UEM sind. Die Erzwingungsaktion wird auf BlackBerry Dynamics-Apps angewendet. Die Einstellung „Basiskonnektivitätsintervall für Authentifikator-Apps“ gibt an, dass die Konnektivitätsprüfung darauf basiert, wann eine Authentifikator-App eine Verbindung zu UEM herstellt. Diese Einstellung gilt nur, wenn ein Authentifikator in einem BlackBerry Dynamics-Profil angegeben ist. Die Einstellung „Letzte Kontaktzeit“ gibt die Anzahl der Tage an, die ein Gerät ohne Kontakt zu UEM sein kann, bevor das Gerät als nicht mehr kompatibel angesehen wird. BlackBerry Dynamics-Apps fordern Benutzer nicht zur Einhaltung dieser Regel auf. Wenn Sie die Einstellung „Verhalten der Eingabeaufforderung“ auf „Nach Konformität fragen“ setzen, wird der Benutzer nicht aufgefordert. Wenn das Gerät in der Lage ist, UEM zu kontaktieren, kehrt das Gerät zur Konformität zurück, wenn der Benutzer die BlackBerry Dynamics-App öffnet.
Erkennung von Bildschirmerfassung auf iOS-Geräten durch BlackBerry Dynamics	Diese Einstellung erstellt eine Konformitätsregel, die auf Bildschirmerfassungen von BlackBerry Dynamics-Apps auf Geräten reagiert. Die Einstellung „Maximale Anzahl von Bildschirmerfassungen innerhalb eines Zeitraums“ gibt die Anzahl der zulässigen Bildschirmerfassungen innerhalb einer festgelegten Zeit an. Die Einstellung „Erzwingungsaktion für BlackBerry Dynamics-Apps“ gibt die Aktion an, die ausgeführt wird, wenn der Benutzer die zulässige Anzahl von Bildschirmerfassungen überschreitet.
Eine gesperrte App wurde installiert	Diese Einstellung erstellt eine Konformitätsregel für UEM, die eine regelmäßige Suche nach gesperrten Apps beinhaltet. Fügen Sie Apps zur Liste der gesperrten Apps im Profil hinzu, indem Sie die Apps aus der Liste der von UEM gesperrten Apps auswählen oder indem Sie eine integrierte App auswählen (nur überwachte Geräte). Wenn Sie diese Einstellung auswählen und eine gesperrte App auf einem Gerät installiert ist, werden eine Warnmeldung und ein Link auf dem Bildschirm „Verwaltete Geräte“ in der Konsole angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der Apps angezeigt, die das Gerät in einen nicht richtlinienkonformen Zustand versetzen. Die Liste der gesperrten Apps wird auch in der Benachrichtigung zur Vorschrifteneinhaltung an den Benutzer gesendet. Bei 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.

Einstellung für Konformitätsprofil	Beschreibung
Nur zulässige Apps auf dem Gerät zeigen	Durch diese Einstellung wird eine Konformitätsregel erstellt, die eine Liste mit Apps festlegt, die auf Geräten installiert werden können. Alle anderen Apps sind nicht zulässig. Fügen Sie Apps zur Liste der zulässigen Apps im Profil hinzu, indem Sie Apps aus der Liste der UEM-Apps auswählen oder indem Sie integrierte Apps auswählen. Einige Apps sind standardmäßig in der Liste zulässiger Apps enthalten. Diese Einstellung ist nur für Geräte unter Aufsicht gültig.

macOS: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der Erzwingungsaktionen, die BlackBerry UEM ausführen kann, wenn ein Gerät eine Konformitätsregel verletzt.

Einstellung für Konformitätsprofil	Beschreibung
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten keine gesperrten Betriebssystemversionen installiert werden. 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 zu sperren. 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.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliothekversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.
Überprüfung der BlackBerry Dynamics-Verbindung	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu überwachen, ob BlackBerry Dynamics-Apps länger als eine angegebene Zeitspanne ohne Kontakt zu UEM sind. Die Erzwingungsaktion wird auf BlackBerry Dynamics-Apps angewendet. Die Einstellung „Basiskonnektivitätsintervall für Authentifikator-Apps“ gibt an, dass die Konnektivitätsprüfung darauf basiert, wann eine Authentifikator-App eine Verbindung zu UEM herstellt. Diese Einstellung gilt nur, wenn ein Authentifikator in einem BlackBerry Dynamics-Profil angegeben ist. Die Einstellung „Letzte Kontaktzeit“ gibt die Anzahl der Tage an, die ein Gerät ohne Kontakt zu UEM sein kann, bevor das Gerät als nicht mehr kompatibel angesehen wird.

Android: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der Erzwingungsaktionen, die BlackBerry UEM ausführen kann, wenn ein Gerät eine Konformitätsregel verletzt.

Einstellung für Konformitätsprofil	Beschreibung
Gerootetes Betriebssystem oder Fehler bei Knox-Nachweis	Mit dieser Einstellung wird eine Konformitätsregel für die Aktionen erstellt, die ausgeführt werden, wenn ein Benutzer oder Angreifer Zugriff auf die Root-Ebene eines Android-Geräts erhält. Wenn Sie diese Einstellung auswählen, können Benutzer keine neuen Aktivierungen für gerootete Geräte durchführen, unabhängig von der von Ihnen festgelegten Erzwingungsaktion. Durch Auswahl von „Anti-Debugging für BlackBerry Dynamics-Apps aktivieren“ werden BlackBerry Dynamics-Apps gestoppt, wenn die BlackBerry Dynamics-Runtime ein aktives Debugging-Tool erkennt.
Fehlgeschlagener SafetyNet- oder Play Integrity-Nachweis	Mit dieser Einstellung wird eine Konformitätsregel für die Aktionen erstellt, die ausgeführt werden, wenn der SafetyNet- oder Play Integrity-Nachweis bei einem Gerät nicht erbracht werden kann. Wenn Sie SafetyNet- oder Play Integrity-Nachweise verwenden, sendet UEM Abfragen zum Testen der Authentizität und der Integrität von Android-Geräten und -Apps in der Umgebung Ihres Unternehmens. Siehe Verwalten des Nachweises für Android-Geräte und BlackBerry Dynamics-Apps.
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 ist, werden eine Warnmeldung und ein Link auf dem Bildschirm „Verwaltete Geräte“ in der Konsole angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der nicht zugewiesenen Apps angezeigt. Auf Android Enterprise-, Android Management- 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 auf einem Android-Gerät nicht installiert ist, werden eine Warnmeldung und ein Link auf dem Bildschirm „Verwaltete Geräte“ in der Konsole angezeigt. Für Android Enterprise- und Android Management-Apps gelten die Erzwingungsaktionen nicht. Auf Samsung Knox-Geräten werden die erforderlichen internen Apps automatisch installiert. Die Erzwingungsaktionen gelten nur für erforderliche öffentliche Apps.

Einstellung für Konformitätsprofil	Beschreibung
Gesperrte Betriebssystemversion wurde installiert	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass auf Geräten keine gesperrten Betriebssystemversionen installiert werden. 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 zu sperren. Sie können die Gerätemodelle angeben, 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 Konformitätsregel erstellt, um zu überwachen, ob Geräte länger als eine angegebene Zeitspanne lang ohne Kontakt zu UEM sind. Die Einstellung „Letzte Kontaktzeit“ gibt die Anzahl der Tage an, die ein Gerät ohne Kontakt zu UEM sein kann, bevor das Gerät nicht mehr kompatibel ist.
Erforderliche Security Patch-Stufe nicht installiert	Durch diese Einstellung wird eine Konformitätsregel erstellt, um zu gewährleisten, dass auf Geräten die erforderlichen Sicherheitspatches installiert sind. Sie können die Gerätemodelle angeben, auf denen Sicherheitspatches installiert sein müssen, sowie ein Datum für das Sicherheitspatch. Geräte mit einem Sicherheitspatch, dessen Datum dem angegebenen Datum entspricht oder nach diesem liegt, gelten als konform. Sofern Sie zuvor ein Konformitätsprofil erstellt haben, für das die Einstellung „Erforderliche Security Patch-Stufe ist nicht installiert“ aktiviert ist, wird die Erzwingungsaktion nach einem Upgrade auf „Überwachen und Protokollieren“ gesetzt.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliothekversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.
Überprüfung der BlackBerry Dynamics-Verbindung	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um zu überwachen, ob BlackBerry Dynamics-Apps länger als eine angegebene Zeitspanne ohne Kontakt zu UEM sind. Die Erzwingungsaktion wird auf BlackBerry Dynamics-Apps angewendet. Die Einstellung „Basiskonnektivitätsintervall für Authentifikator-Apps“ gibt an, dass die Konnektivitätsprüfung darauf basiert, wann eine Authentifikator-App eine Verbindung zu UEM herstellt. Diese Einstellung gilt nur, wenn ein Authentifikator in einem zugewiesenen BlackBerry Dynamics-Profil angegeben ist. Die Einstellung „Letzte Kontaktzeit“ gibt die Anzahl der Tage an, die ein Gerät ohne Kontakt zu UEM sein kann, bevor davon ausgegangen wird, dass es nicht mehr kompatibel ist.

Einstellung für Konformitätsprofil	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- und Android Management-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. Wählen Sie für Geräte mit der Aktivierungsart Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) die Option „Konformität im persönlichen Bereich erzwingen“ aus, um die Regel auf Apps im geschäftlichen und im persönlichen Profil anzuwenden. Diese Einstellung gilt nicht für Geräte mit Privatsphäre des Benutzers-Aktivierung. Wenn Sie diese Einstellung auswählen und eine gesperrte App auf einem Android-Gerät installiert ist, werden eine Warnmeldung und ein Link auf dem Bildschirm „Verwaltete Geräte“ in der Konsole angezeigt. Wenn Sie auf den Link klicken, wird eine Liste der gesperrten Apps angezeigt.
Das Kennwort erfüllt nicht die Komplexitätsanforderunge	Durch diese Einstellung wird eine Konformitätsregel erstellt, um sicherzustellen, dass der Benutzer Kennwörter für das Gerät und den geschäftlichen Bereich festgelegt hat, die die Komplexitätsanforderungen erfüllen, die in den zugewiesenen IT-Unternehmensrichtlinien festgelegt sind.

Windows: Kompatibilitätsprofil-Einstellungen

Unter Allgemein: Einstellungen für Kompatibilitätsprofil finden Sie Beschreibungen der Erzwingungsaktionen, die BlackBerry UEM ausführen kann, wenn ein Gerät eine Konformitätsregel verletzt.

Einstellung für Konformitätsprofil	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 keine gesperrten Betriebssystemversionen installiert werden. Sie können die gesperrten Betriebssystemversionen auswählen.
Gesperrtes Gerätemodell gefunden	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um Gerätemodelle zu sperren. Sie können die Gerätemodelle auswählen, die zugelassen oder gesperrt sind.

Einstellung für Konformitätsprofil	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 UEM sind.
Überprüfung der BlackBerry Dynamics-Bibliotheksversion	Mit dieser Einstellung wird eine Konformitätsregel erstellt, mit der Sie die BlackBerry Dynamics-Bibliothekversionen auswählen können, die nicht aktiviert werden können. Sie können die gesperrten Bibliotheksversionen auswählen.
Überprüfung der BlackBerry Dynamics-Verbindung	Durch diese Einstellung wird eine Kompatibilitätsregel erstellt, um sicherzustellen, dass BlackBerry Dynamics-Apps nicht länger als eine angegebene Zeitspanne lang ohne Kontakt zu 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 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.
Integritätsnachweis für Windows-Geräte	
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 Datenausführungsverhinde 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.

Einstellung für Konformitätsprofil	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. Sie geben die erwartete Version an.
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. Sie geben die erwartete Version an.
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. Sie geben die zulässigen Werte an.

Einstellung für Konformitätsprofil	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. Sie geben die zulässigen Werte an.
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. Sie geben die zulässigen Werte an.

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 zuteilen möchten, 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 sein 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 Benutzer und Geräte

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Senden eines Befehls an einen bestimmten Benutzer oder ein bestimmtes Gerät	**a.** Suchen Sie nach einem Benutzer, und klicken Sie darauf. **b.** Klicken Sie auf der Registerkarte Gerät im Abschnitt **Gerät verwalten** auf den entsprechenden Befehl.
Senden eines Stapelbefehls an mehrere Benutzer oder Geräte	**a.** Suchen Sie mehrere Benutzer, und wählen Sie sie aus. **b.** Klicken Sie im Befehlsmenü über der Benutzerliste auf den entsprechenden Befehl.

Weitere Informationen zu den verfügbaren Befehlen finden Sie an folgenden Stellen:

- Befehle für iOS- und iPadOS-Geräte.
- Befehle für macOS-Geräte.
- Befehle für Android-Geräte.
- Befehle für Windows-Geräte.

Wenn Sie fertig sind: Wenn Sie für die Befehle „Alle Gerätedaten löschen“ und „Nur geschäftliche Daten löschen“ einen Ablaufdatum festlegen möchten, siehe Festlegen einer Ablaufzeit für Befehle.

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 UEM herstellen kann, bleibt der Befehl im Status „Ausstehend“, und das Gerät wird nicht aus

UEM entfernt, es sei denn, Sie entfernen es manuell. Alternativ können Sie UEM so konfigurieren, dass Geräte automatisch entfernt werden, wenn Befehle nach einem bestimmten Zeitraum nicht ausgeführt wurden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Ablauf des Befehls zum Löschen**.
2. Wählen Sie für einen oder beide Befehle die Option **Gerät automatisch entfernen, wenn der Befehl abläuft**.
3. Geben Sie im Feld **Ablauf des Befehls** die Anzahl der Tage ein, nach denen der Befehl abläuft und das Gerät automatisch aus UEM entfernt wird.
4. Klicken Sie auf **Speichern**.

Befehle für iOS- und iPadOS-Geräte

Befehl	Beschreibung	Aktivierungsarten
Anzeigen des Geräteberichts	Durch diesen Befehl werden Detailinformationen zu einem Gerät angezeigt. Sie können den Gerätebericht exportieren und speichern.	MDM-Steuerelemente Privatsphäre des Benutzers
Anzeigen der Geräteaktionen	Mit diesem Befehl werden alle Aktionen angezeigt, die gerade auf einem Gerät durchgeführt werden.	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 UEM herstellt, nachdem Sie es entfernt haben, werden nur die Geschäftsdaten vom Gerät entfernt. Wenn eSIM-Informationen auf einem oder mehreren von Ihnen ausgewählten Geräten erkannt werden, werden Sie aufgefordert anzugeben, ob die Datentarifinformationen beibehalten werden müssen.	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 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 UEM herstellt, nachdem Sie es entfernt haben, werden die geschäftlichen Daten vom Gerät entfernt.	MDM-Steuerelemente Privatsphäre des Benutzers

Befehl	Beschreibung	Aktivierungsarten
Gerät sperren	Mit diesem Befehl sperren Sie ein Gerät. Apple fügt „Verlorenes iPhone“ oder „Verlorenes iPad“ zum Titel Ihrer Nachricht hinzu. Der Benutzer muss das bestehende Gerätekennwort eingeben, um das Gerät zu entsperren. Wenn Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Kennwort entsperren und löschen	Dieser Befehl entsperrt ein Gerät und löscht das bestehende Kennwort. Der Benutzer wird zur Eingabe eines Gerätekennworts aufgefordert. Sie können diesen Befehl verwenden, wenn der Benutzer das Gerätekennwort vergessen hat. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Verloren-Modus aktivieren	Durch diesen Befehl wird das Gerät gesperrt, und Sie können eine Telefonnummer und eine Nachricht auf dem Gerät anzeigen. Nachdem Sie diesen Befehl gesendet haben, können Sie den Standort des Geräts in der Verwaltungskonsole anzeigen. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
BlackBerry 2FA deaktivieren	Mit diesem Befehl werden Geräte deaktiviert, die mit der Aktivierungsart BlackBerry 2FA aktiviert wurden. Das Gerät wird von 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. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Gerät neu starten	Dieser Befehl erzwingt den Neustart des Geräts. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente
Gerät abschalten	Dieser Befehl erzwingt das Ausschalten des Geräts. Diese Option wird nur für Geräte unter Aufsicht unterstützt. Dieser Befehl wird für Apple TV-Geräte nicht unterstützt.	MDM-Steuerelemente

Befehl	Beschreibung	Aktivierungsarten
Apps bereinigen	Mit diesem Befehl werden die Daten von allen mit Microsoft Intune verwalteten Apps auf dem Gerät bereinigt. Die Apps werden nicht vom Gerät entfernt.	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.	MDM-Steuerelemente Privatsphäre des Benutzers
Zeitzone aktualisieren	Mit diesem Befehl wird die Zeitzone des Geräts entsprechend der ausgewählten Region festgelegt.	MDM-Steuerelemente
Gerät entfernen	Dieser Befehl entfernt das Gerät aus 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, UEM zu kontaktieren versucht, erhält der Benutzer eine Benachrichtigung. Das Gerät kann erst dann wieder mit UEM kommunizieren, wenn es erneut aktiviert wurde.	MDM-Steuerelemente Privatsphäre des Benutzers
Aktualisieren von eSIM-Mobilfunkverträgen	Bei Geräten mit einem eSIM-basierten Mobilfunkvertrag fragt dieser Befehl aktualisierte Vertragsdetails für das Gerät über die Betreiber-URL des Geräts ab.	MDM-Steuerelemente

Befehle für macOS-Geräte

Befehl	Beschreibung
Anzeigen des Geräteberichts	Durch diesen Befehl werden Detailinformationen zu einem Gerät angezeigt. Sie können den Gerätebericht exportieren und speichern.
Anzeigen der Geräteaktionen	Mit diesem Befehl werden alle Aktionen angezeigt, die gerade auf einem Gerät durchgeführt werden.
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.

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 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.
Gerät entfernen	Dieser Befehl entfernt das Gerät aus UEM. Das Gerät empfängt ggf. weiterhin E-Mails und andere geschäftliche Daten.

Befehle für Android-Geräte

Informationen zu Android Management-Aktivierungsarten finden Sie unter Überlegungen zu Aktivierungsarten für Android Management.

Befehl	Beschreibung	Aktivierungsarten
Anzeigen des Geräteberichts	Durch diesen Befehl werden Detailinformationen zu einem Gerät angezeigt. Sie können den Gerätebericht exportieren und speichern.	Alle (außer BlackBerry 2FA)
Anzeigen der Geräteaktionen	Mit diesem Befehl werden alle Aktionen angezeigt, die gerade auf einem Gerät durchgeführt werden.	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 Sie diesen Befehl senden, wird das Gerät nur gesperrt, wenn ein Gerätekennwort vorhanden ist. Andernfalls wird auf dem Gerät keine Aktion ausgeführt.	Geschäftlich und persönlich – vollständige Kontrolle (Android Management) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Management) Nur geschäftlicher Bereich (Android Management) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Nur geschäftlicher Bereich (Android Enterprise) MDM-Steuerelemente

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 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 UEM herstellt, nachdem es entfernt wurde, werden nur die Geschäftsdaten vom Gerät gelöscht. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	Geschäftlich und persönlich – vollständige Kontrolle (Android Management) Nur geschäftlicher Bereich (Android Management) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Nur geschäftlicher Bereich - (Samsung Knox) MDM-Steuerelemente
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, wird der Bereich selbst vom Gerät gelöscht, aber alle persönlichen Apps und Daten bleiben. Wenn Sie diesen Befehl auf Android Enterprise-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 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 UEM herstellt, nachdem es gelöscht wurde, werden die Geschäftsdaten vom Gerät entfernt. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.	Geschäftlich und persönlich – vollständige Kontrolle (Android Management) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Management) Geschäftlich und persönlich – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox) Nur geschäftlicher Bereich (Samsung Knox) MDM-Steuerelemente

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. Dieser Befehl wird auf Geräten mit Samsung Knox SDK 3.2.1 oder höher nicht unterstützt.	Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox) Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox) MDM-Steuerelemente (nur Samsung-Geräte)
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.	Geschäftlich und persönlich – Benutzer-Datenschutz (Android Management) Nur geschäftlicher Bereich (Android Management) Nur geschäftlicher Bereich (Android Enterprise) Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)
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	Mit diesem Befehl können Sie 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 – vollständige Kontrolle (Android Enterprise) Geschäftlich und persönlich – Benutzer-Datenschutz (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 (Android Management) Geschäftlich und persönlich – Benutzer-Datenschutz (Android Management) Nur geschäftlicher Bereich (Android Management) 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 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 mit Microsoft Intune verwalteten Apps auf dem Gerät bereinigt. Die Apps werden nicht vom Gerät entfernt.	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.	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 Management) Nur geschäftlicher Bereich (Android Enterprise)

Befehl	Beschreibung	Aktivierungsarten
Gerät entfernen	Dieser Befehl entfernt das Gerät aus 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, UEM zu kontaktieren versucht, erhält der Benutzer eine Benachrichtigung. Das Gerät kann erst dann wieder mit UEM kommunizieren, wenn es erneut aktiviert wurde.	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 speichern.
Anzeigen der Geräteaktionen	Mit diesem Befehl werden alle Aktionen angezeigt, die gerade auf einem Gerät durchgeführt werden.
Gerät sperren	Mit diesem Befehl sperren Sie ein Gerät. Der Benutzer muss das bestehende Gerätekennwort eingeben, um das Gerät zu entsperren. 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 UEM löschen. Wenn das Gerät keine Verbindung zu UEM herstellen kann, können Sie es aus UEM löschen. Wenn das Gerät eine Verbindung zu UEM herstellt, nachdem es entfernt wurde, werden nur die Geschäftsdaten vom Gerät gelöscht. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.
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 UEM. Nachdem Sie diesen Befehl gesendet haben, können Sie das Gerät optional aus UEM löschen. Wenn das Gerät keine Verbindung zu UEM herstellen kann, können Sie es aus UEM löschen. Wenn das Gerät eine Verbindung zu UEM herstellt, nachdem es entfernt wurde, werden nur die Geschäftsdaten vom Gerät gelöscht. Falls zutreffend, wird auch der geschäftliche Bereich entfernt.
Desktop/Gerät neu starten	Dieser Befehl erzwingt den Neustart des Geräts.
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.
Gerät entfernen	Dieser Befehl entfernt das Gerät aus UEM. Das Gerät empfängt ggf. weiterhin E-Mails und andere geschäftliche Daten.

Steuern, wie Softwareupdates auf Geräten installiert werden

Sie können Profile für Gerätedienstanforderungen verwenden, um zu steuern, wie Gerätesoftware-Updates auf Android Enterprise-, Android Management- und Samsung Knox-Geräten installiert werden und wie App-Updates für im Vordergrund ausgeführte Apps verwaltet werden.

Sie können die auf iOS-Geräten installierten Softwareversionen nicht steuern, aber Sie können die Installation eines verfügbaren Updates auf iOS-Geräten unter Aufsicht erzwingen.

Erstellen eines Profils für Gerätedienstanforderungen für Android Enterprise- und Android Management-Geräte

Regeln für Betriebssystemaktualisierungen gelten nur für Android Enterprise- und Android Management-Geräte mit den Aktivierungsarten Nur geschäftlicher Bereich und Geschäftlich und persönlich – vollständige Kontrolle. App-Aktualisierungsregeln gelten für alle Android Enterprise-Geräte. Derzeit werden das Aussetzen von Betriebssystemaktualisierungen und automatischen App-Aktualisierungen für Android Management-Geräte nicht unterstützt. Siehe Überlegungen zu Aktivierungsarten für Android Management.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Konformität > Gerätedienstanforderungen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie zum Konfigurieren der Regeln für Betriebssystemaktualisierungen für Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Geräte im Abschnitt **Regel für Betriebssystemaktualisierungen** auf + und tun Sie Folgendes:
   a) Wählen Sie in der Drop-down-Liste **Gerätemodell** ein Gerätemodell aus.
   b) Wählen Sie in der Drop-down-Liste **Betriebssystemversion** die installierte Betriebssystemversion aus.
   c) Wählen Sie in der Dropdown-Liste **Aktualisierungsregel** eine der folgenden Optionen aus:
      - **Standard**: Der Benutzer kann auswählen, wann Updates installiert werden sollen. Benutzer mit der Aktivierungsart Nur geschäftlicher Bereich (vollständig verwaltetes Gerät) können nicht auswählen, wann Updates installiert werden.
      - **Automatisch aktualisieren**: Updates werden ohne Aufforderung des Benutzers installiert.
      - **Automatisch aktualisieren zwischen**: Updates werden in einem von Ihnen festgelegten Zeitraum installiert, ohne dass der Benutzer dazu aufgefordert wird. Der Benutzer hat die Wahlmöglichkeit, Updates außerhalb dieses Zeitfensters zu installieren.
      - **Verschieben um bis zu 30 Tage**: Sperren Sie die Installation von Updates für 30 Tage. Nach 30 Tagen kann der Benutzer auswählen, wann ein Update installiert werden soll. Je nach Gerätehersteller und Mobilfunkanbieter werden Sicherheitsupdates möglicherweise nicht verschoben.
   d) Klicken Sie auf **Hinzufügen**.
5. Um Zeiträume anzugeben, in denen keine Betriebssystemaktualisierungen für Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Geräte durchgeführt werden sollen, klicken Sie im Abschnitt **Betriebssystemaktualisierung aussetzen** auf +. Wählen Sie den Monat und den Tag aus, an dem der Aussetzungszeitraum beginnt, sowie die Dauer des Aussetzungszeitraums.

   Wenn Sie mehr als einen Aussetzungszeitraum angeben, müssen zwischen den Zeiträumen mindestens 60 Tage liegen.

6. Wenn Sie einen Aktualisierungszeitraum für Apps festlegen möchten, die im Vordergrund ausgeführt werden, wählen Sie **Updatezeitraum für im Vordergrund laufende Apps aktivieren**. Wählen Sie Startzeit und Dauer.
7. Um festzulegen, wie Google Play die Änderungen auf Apps anwendet, die im Vordergrund ausgeführt werden (die Einstellung „Apps automatisch aktualisieren" in Google Play), wählen Sie in der Dropdown-Liste **Richtlinie für automatische App-Updates** eine der folgenden Optionen aus:

   - **Immer**: Apps werden immer aktualisiert. Apps, die immer laufen (z. B. BlackBerry UEM Client, BlackBerry Work oder BlackBerry Connectivity), werden erst dann aktualisiert, wenn der Benutzer die Aktualisierung manuell durchführt, es sei denn, Sie wählen die Option **Updatezeitraum für im Vordergrund laufende Apps aktivieren** aus.
   - **Nur Wi-Fi**: Apps werden nur dann aktualisiert, wenn das Gerät mit einem Wi-Fi-Netzwerk verbunden ist. Apps, die immer laufen (z. B. UEM Client, BlackBerry Work oder BlackBerry Connectivity), werden erst dann aktualisiert, wenn der Benutzer die Aktualisierung manuell durchführt, es sei denn, Sie wählen die Option **Updatezeitraum für im Vordergrund laufende Apps aktivieren** aus.
   - **Benutzer kann zustimmen**: Der Benutzer wird aufgefordert, die Aktualisierung von Apps auf dem Gerät zuzulassen.
   - **Deaktivieren**: Apps werden nie aktualisiert.

   Wenn Sie **Immer**, **Nur Wi-Fi** oder **Deaktivieren** wählen, kann der Benutzer keine andere Option auf dem Gerät auswählen. Benutzer können Apps weiterhin manuell in Google Play aktualisieren.
8. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.
- Um eine Liste der Benutzer anzuzeigen, die eine gesperrte Softwareversion ausführen (eine Softwareversion, die nicht mehr von einem Dienstanbieter akzeptiert wird), klicken Sie unter **Richtlinien und Profile > Konformität > Gerätedienstanforderungen** auf ein Profil. Klicken Sie dann auf die Registerkarte **x Benutzer mit einer gesperrten Softwareversion**.

Erstellen eines Profils für Gerätedienstanforderungen für Samsung Knox-Geräte

Auf Samsung Knox-Geräten können Sie Knox E-FOTA One (Enterprise Firmware Over the Air) verwenden, um zu steuern, wann Firmware-Aktualisierungen von Samsung installiert werden. Wenn Ihr Unternehmen Samsung E-FOTA (seit 31. Juli 2022 nicht mehr unterstützt) verwendet und Sie auf E-FOTA One migrieren müssen, lesen Sie KB 69901.

Samsung Knox-Geräte, die als Nur geschäftlicher Bereich (Samsung Knox), Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox), Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät) und Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil) aktiviert werden, unterstützen Softwareeinschränkungen mit E-FOTA One.

E-FOTA One wird für die Aktivierungsarten Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox) oder Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise mit geschäftlichem Profil) nicht unterstützt.

Bevor Sie beginnen:

- Gehen Sie in der Menüleiste der Verwaltungskonsole zu **Einstellungen > Lizenzübersicht**, um eine E-FOTA-Lizenz zu BlackBerry UEM hinzuzufügen.
- Um E-FOTA zu verwenden, müssen Sie die globale Android-Regel „OTA-Aktualisierungen zulassen" in der IT-Richtlinie aktivieren, die Sie Geräten zuweisen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Konformität > Gerätedienstanforderungen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Wenn Sie zulassen möchten, dass Android OS-Aktualisierungsregeln auf Samsung-Geräte angewendet werden, wählen Sie das Kontrollkästchen **Einschränkung auf alle Android-Geräte anwenden**.

   Die Firmwareregeln, die Sie in den folgenden Schritten konfigurieren, haben Vorrang vor diesen Regeln. Einstellungen für „Betriebssystemaktualisierung aussetzen“ gelten nicht für Samsung Knox-Geräte, die E-FOTA verwenden.
5. Klicken Sie im Abschnitt **Firmware-Regeln für Samsung-Geräte** auf +.
6. Geben Sie in der Dropdown-Liste **Gerätemodell** das Gerätemodell ein, oder wählen Sie ein Modell aus der Liste aus.
7. Wählen Sie in der Dropdown-Liste **Sprache** eine Sprache aus.
8. Tippen Sie im Feld **Netzbetreibercode** den CSC-Code für den Mobilfunkanbieter ein.
9. Klicken Sie auf **Firmwareversion abrufen**.
10. Wiederholen Sie die zuvor genannten Schritte für jede Firmwareregel, die Sie hinzufügen möchten.
11. Tippen Sie auf **Hinzufügen**, wenn Sie fertig sind.
12. Wenn Sie eine erzwungene Aktualisierung planen möchten, klicken Sie neben der hinzugefügten Firmwareversion auf **Zeitplan**. 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.
    b) Geben Sie in den Dropdown-Listen **Erzwungene Aktualisierung planen in der Zeit von** an, wann die erzwungene Aktualisierung installiert werden muss.

    Wenn Sie eine erzwungene Aktualisierung planen, ist das Knox-Gerät nicht mehr auf die Firmware-Version beschränkt, und Sie können es manuell aktualisieren, wenn eine neuere Version verfügbar ist.
13. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.
- Um eine Liste der Benutzer anzuzeigen, die eine gesperrte Softwareversion ausführen (eine Softwareversion, die nicht mehr von einem Dienstanbieter akzeptiert wird), klicken Sie unter **Richtlinien und Profile > Konformität > Gerätedienstanforderungen** auf ein Profil. klicken Sie dann auf die Registerkarte **x Benutzer mit einer gesperrten Softwareversion**.

Aktualisieren des Betriebssystems auf einem beaufsichtigten iOS-Gerät

Sie können die Installation eines verfügbaren Betriebssystem-Updates auf einem iOS-Gerät erzwingen. Informationen zur Aktualisierung des Betriebssystems auf mehreren Geräten gleichzeitig finden Sie unter Senden von Befehlen an Benutzer und Geräte. Sie können die zeitliche Planung von iOS-Softwareupdates mithilfe der IT-Richtlinienregeln „Verzögerung von Softwareupdates“ und „Verzögerungszeit für Softwareupdates“ steuern.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach dem Namen eines Benutzerkontos, und klicken Sie darauf.
3. Wenn ein Softwareupdate verfügbar ist, klicken Sie in der entsprechenden Registerkarte „Geräte“ auf **Jetzt aktualisieren**.

4. 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.
5. Wählen Sie in der Liste **Betriebssystemversion** die Betriebssystemversion aus, auf die Sie das Gerät aktualisieren möchten.
6. Klicken Sie auf **Aktualisieren**.

Konfigurieren, wie Geräte BlackBerry UEM kontaktieren, um App- und Konfigurationsaktualisierungen zu erhalten

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 UEM das Gerät dazu auf, 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 UEM in einem von Ihnen festgelegten Intervall kontaktiert.

In lokalen Umgebungen können Sie außerdem das Enterprise Management Agent-Profil verwenden, um UEM zu erlauben, eine Liste von persönlichen Apps auf den Geräten von Benutzern zu erfassen.

Erstellen eines Enterprise Management Agent-Profils

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Richtlinie > Enterprise Management Agent**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Konfigurieren Sie die Einstellungen für das jeweilige Gerät. Weitere Informationen zu den Einstellungen finden Sie an folgenden Stellen:
   - iOS: Enterprise Management Agent-Profileinstellungen
   - Android: Enterprise Management Agent-Profileinstellungen
   - Windows: Enterprise Management Agent-Profileinstellungen
5. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.

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 geöffnet ist.
Sammlung von persönlichen Apps zulassen	Legen Sie fest, ob BlackBerry UEM eine Liste mit persönlichen Apps enthält, die auf dem Gerät 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.
Akku-Grenzwert	Geben Sie den Grenzwert für den Akku-Ladestand in Prozent an, der erforderlich ist, bevor das Gerät Informationen an BlackBerry UEM sendet.
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 UEM erforderlich ist.
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 UEM erforderlich ist.
Grenzwert für Speicherkarte	Legen Sie den Grenzwert für den externen freien Speicherplatz in Megabytes fest, der vor dem Zurücksenden von Informationen vom Gerät an UEM erforderlich ist.
Enterprise Management Agent-Abfragerate	Geben Sie in Sekunden an, wie häufig das Gerät Enterprise Management Agent-Serverbefehle abruft.
Sammlung von persönlichen Apps zulassen	Legen Sie fest, ob UEM eine Liste mit persönlichen Apps enthält, die auf dem Gerät 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.

Einstellung	Beschreibung
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	Legen Sie fest, ob BlackBerry UEM eine Liste mit persönlichen Apps enthält, die auf dem Gerät der Benutzer installiert sind.

Anzeigen von Organisationsinformationen auf Geräten

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

Bei iOS-, macOS-, Android- und Windows 10-Geräten können Sie benutzerdefinierte Organisationshinweise erstellen, die während des Aktivierungsprozesses angezeigt werden (Sie können beispielsweise einen Hinweis zu den Bedingungen anzeigen, 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 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. Bei iOS- und Android-Geräten werden Unternehmensinformationen auf dem BlackBerry UEM Client 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 Samsung Knox-Geräten können Sie das Geräteprofil verwenden, um den benutzerdefinierten Organisationshinweis anzuzeigen, wenn der Benutzer das Gerät startet.

Bei Samsung Knox- und überwachten iOS-Geräten können Sie das Geräteprofil auch zum Hinzufügen eines benutzerdefinierten Hintergrundbildes 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 Samsung Knox-Geräten wird der Hintergrund im geschäftlichen Bereich angezeigt.

Geräteprofile werden nicht für iOS-Geräte unterstützt, die mit einer Aktivierungsart für Benutzerdatenschutz aktiviert wurden.

Erstellen von Organisationshinweisen

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Organisationshinweise**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen für den Organisationshinweis ein.
4. Optional können Sie auch den Text aus einem bereits vorhandenen Organisationshinweis übernehmen, indem Sie ihn in der Dropdown-Liste **Kopierter Text aus Organisationshinweis** auswählen.
5. Wählen Sie in der Dropdown-Liste **Gerätesprache** die Standardsprache für den Hinweis aus.
6. Geben Sie im Feld **Organisationshinweis** den Inhalt des Hinweises ein.
7. Klicken Sie optional bei Bedarf auf **Hinzufügen einer weiteren Sprache** klicken, um den Organisationshinweis in mehreren Sprachen zu posten.
8. Wenn Sie den Organisationshinweis in mehr als einer Sprache veröffentlichen, wählen Sie die Option **Standardsprache** unter einer der Nachrichten, um die Standardsprache festzulegen.
9. 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.

Erstellen eines Geräteprofils

Bevor Sie beginnen: Folgen Sie für Samsung Knox-Geräte den Anweisungen unter Erstellen von Organisationshinweisen.

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

Aufgabe	Schritte
Weisen Sie einen Organisationshinweis zu, der auf Samsung Knox-Geräten angezeigt wird, wenn ein Benutzer sein Gerät neu startet.	Wählen Sie auf der Registerkarte **Android** in der Dropdown-Liste **Organisationshinweis zuweisen** den entsprechenden Organisationshinweis aus.
Definieren Sie für iOS- und Android-Geräte die Unternehmensinformationen, die im BlackBerry UEM Client angezeigt werden sollen. Definieren Sie für Windows 10 die Telefonnummer und E-Mail-Adresse, die in den Support-Informationen auf Geräten angezeigt werden sollen.	Geben Sie auf der entsprechenden Registerkarte des Betriebssystems den Namen, die Adresse, die Telefonnummer und die E-Mail-Adresse an.

5. Führen Sie optional einen der folgenden Schritte aus:

Aufgabe	Schritte
Hinzufügen eines Hintergrundbilds zum geschäftlichen Bereich auf Samsung Knox-Geräten.	**a.** Klicken Sie auf der Registerkarte **Android** im Bereich **Hintergrundbild für den geschäftlichen Bereich** auf **Durchsuchen**. **b.** Navigieren Sie zu dem Bild, und wählen Sie es aus.
Hinzufügen eines Hintergrundbilds bei überwachten iOS-Geräten.	**a.** Wählen Sie auf der Registerkarte **iOS** im Abschnitt **Hintergrundbild des Geräts** in der Dropdown-Liste **Hintergrundbild festlegen für** aus, wo das Bild angezeigt werden soll. **b.** Klicken Sie auf **Durchsuchen**. **c.** Navigieren Sie zu dem Bild, und wählen Sie es aus.

6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.

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. Sie 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.

Gehen Sie wie folgt vor, um Standortdienste zu aktivieren und zu verwenden:

Schritt	Aktion
1	Konfigurieren der Einstellungen für die Standortbestimmung.
2	Erstellen eines Profils für die Standortbestimmung.
3	Standort eines Geräts bestimmen.
4	Optional Einschalten des Verloren-Modus für iOS-Geräte unter Aufsicht.

Konfigurieren der Einstellungen für die Standortbestimmung

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Standortdienst**.
2. Geben Sie in einer lokalen Umgebung im Feld **Alter des Standortverlaufs** an, wie lange BlackBerry UEM den Standortverlauf für Geräte speichern soll. Standardmäßig speichert UEM den Verlauf einen Monat lang.
3. Klicken Sie in der Dropdown-Liste **Angezeigte Geschwindigkeitseinheit** auf **km/h** oder**mph**.
4. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Erstellen eines Profils für die Standortbestimmung.

Erstellen eines Profils für die Standortbestimmung

Bevor Sie beginnen: Konfigurieren der Einstellungen für die Standortbestimmung.

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

5. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Aktivieren des Standortverlaufs für iOS-Geräte	Überprüfen Sie auf der Registerkarte **iOS**, ob das Kontrollkästchen **Gerätestandortverlauf protokollieren** aktiviert ist. BlackBerry UEM sammelt 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. Die Bedingungen für die Entfernung und die Häufigkeit müssen erfüllt sein, bevor der Gerätestandort aktualisiert wird.

6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu. 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.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.
- Standort eines Geräts bestimmen.

Standort eines Geräts bestimmen

Bevor Sie beginnen: Erstellen eines Profils für die Standortbestimmung.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Deaktivieren Sie das Kontrollkästchen für jedes Gerät, dessen Standort Sie bestimmen möchten.
3. Klicken Sie auf .
4. Suchen Sie die Geräte auf der Karte mithilfe des Symbols „Aktueller Standort“ ( ) und des Symbols „Letzter Gerätestandort“ ( ). 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.
5. Klicken Sie auf ein Symbol, oder bewegen Sie den Mauszeiger darüber, um Standortinformationen anzuzeigen, z. B. Breiten- und Längengrad und wann der Standort gemeldet wurde.
6. Um den Standortverlauf für iOS- oder Android-Geräte anzuzeigen, klicken Sie auf **Standortverlauf anzeigen**, wählen Sie einen Datums- und Uhrzeitbereich aus, und klicken Sie auf **Senden**.

Einschalten 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, können Sie den Verloren-Modus aktivieren, um das Gerät zu sperren und eine angezeigte Nachricht festzulegen. Außerdem können Sie den aktuellen Standort des Geräts anzeigen, ohne ein Standortdienstprofil zu verwenden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Klicken Sie auf ein Gerät.
3. Klicken Sie auf 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**.

Wenn Sie fertig sind:

- Um ein Gerät zu finden, das sich im Verloren-Modus befindet, klicken Sie auf der Registerkarte „Gerät“ auf **Gerätestandort abrufen**.
- Um den Verloren-Modus zu deaktivieren, klicken Sie auf der Registerkarte „Gerät“ auf **Verloren-Modus deaktivieren**.

Aktivieren der Aktivierungssperre für ein iOS-Gerät

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.

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 für mehrere Geräte mithilfe der zugewiesenen IT-Richtlinienregel aktivieren. Wenn Sie die Aktivierungssperre aktivieren, speichert 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.

Führen Sie die folgenden Schritte durch, um die Aktivierungssperre für jedes Gerät einzeln zu aktivieren.

Bevor Sie beginnen:

- Das Gerät muss überwacht werden.
- Das Gerät muss mit einem iCloud-Konto verknüpft sein.
- Auf dem Gerät muss „Mein iPhone suchen“ oder „Mein iPad suchen“ aktiviert sein.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer**.
2. Suchen Sie nach einem Benutzerkonto, und klicken Sie darauf.
3. Klicken Sie auf der Registerkarte Gerät im Abschnitt **Gerät verwalten** auf **Aktivierungssperre aktivieren**.

Wenn Sie fertig sind:

- Um die Aktivierungssperre für ein Gerät zu deaktivieren, klicken Sie auf **Aktivierungssperre deaktivieren**. Wenn die Aktivierungssperre mithilfe der IT-Richtlinienregel aktiviert wird, können Sie diese Option nicht verwenden, um sie zu deaktivieren.
- Um den Umgehungscode für ein Gerät anzuzeigen, navigieren Sie zu **Benutzer > Apple-Aktivierungssperre**, und suchen Sie dann nach einem Gerät, und klicken Sie darauf.

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. Wenn eine Funktion durch eine vorhandene 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 UEM-Payload-Profilen hinzufügen. Sie können benutzerdefinierte Payload-Profile Benutzern, Benutzergruppen und Gerätegruppen zuweisen.

Sie möchten beispielsweise eine neue Funktion steuern, die auf Geräten nach einem Upgrade auf das neue iOS-Update verfügbar ist, aber UEM verfügt bis zu einer zukünftigen UEM-Softwareversion über kein Profil für die neue Funktion. Um dieses Problem zu lösen, können Sie ein benutzerdefiniertes Payload-Profil erstellen, das diese Funktion steuert, bis sie offiziell von UEM unterstützt wird.

Benutzerdefiniertes Payload-Profil erstellen

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

1. Erstellen Sie im Apple Configurator ein Apple-Konfigurationsprofil.
2. Kopieren Sie 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>
```

3. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Richtlinien und Profile > Benutzerdefiniert > Benutzerdefinierte Payload**.
4. Klicken Sie auf +.
5. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
6. Fügen Sie im Feld **Benutzerdefinierte Payload** den XML-Code ein, den Sie in Schritt 2 kopiert haben.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Profil Benutzern und Gruppen zu.

Verwalten des werkseitigen Rücksetzschutzes für Android Enterprise- und Android Management-Geräte

Sie können das Profil für werkseitigen Rücksetzschutz verwenden, um die Funktion für werkseitigen Rücksetzschutz für die Android Enterprise- und Android Management-Geräte Ihres Unternehmens zu steuern, die mit den Aktivierungsarten Nur geschäftlicher Bereich und Geschäftlich und persönlich – vollständige Kontrolle aktiviert wurden.

Der werkseitige Rücksetzschutz erfordert, dass ein Benutzer des Android-Geräts seine Google-Konto-Anmeldedaten eingibt, um ein Gerät zu entsperren, das auf die Werkseinstellungen zurückgesetzt wurde. Es ist standardmäßig aktiviert, wenn ein Benutzer dem Gerät ein Google-Konto hinzufügt. Mit diesem Profil können Sie den werkseitigen Rücksetzschutz deaktivieren oder ein Benutzerkonto festlegen, mit dem ein Gerät entsperrt werden kann, nachdem es auf die Werkseinstellungen zurückgesetzt wurde.

Profile für werkseitigen Rücksetzschutz bieten die folgenden Optionen:

Option	Beschreibung	Unterstützte Aktivierungsarten
Werkseitigen Rücksetzschutz deaktivieren	Jeder kann ein verloren gegangenes oder gestohlenes Gerät auf die Werkseinstellungen zurücksetzen und mit der Verwendung des Geräts beginnen. Diese Option ist nützlich, wenn ein bekannter Benutzer seine Google-Konto-Anmeldeinformationen vergessen hat oder wenn Sie ein Gerät zurücksetzen müssen, das Ihrem Unternehmen gehört und an Sie zurückgegeben wurde.	Android Enterprise
Vorherige Google-Kontoanmeldedaten aktivieren und verwenden, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird	Benutzer können Google-Konto-Anmeldeinformationen verwenden, die dem Gerät bereits nach dem Zurücksetzen auf die Werkseinstellungen zugeordnet wurden. Dies ist das Standardverhalten. Wenn ein Gerät auf die Werkseinstellungen zurückgesetzt wird, muss sich der Benutzer mit den Google-Konto-Anmeldeinformationen, die sich bereits auf dem Gerät befinden, beim Gerät anmelden. Dadurch wird verhindert, dass jemand mit einem verlorenen oder gestohlenen Gerät das Gerät selbst zurücksetzen und benutzen kann.	Android Enterprise

Option	Beschreibung	Unterstützte Aktivierungsarten
Google-Kontoanmeldedaten aktivieren und angeben, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird	Sie können Google-Konto-Anmeldeinformationen angeben, die ein Benutzer verwenden kann, um sich am Gerät anzumelden, nachdem es auf die Werkseinstellungen zurückgesetzt wurde. Mit dieser Option kann Ihr Unternehmen steuern, wer sich bei einem Gerät anmelden kann, nachdem es auf die Werkseinstellungen zurückgesetzt wurde. BlackBerry empfiehlt, diese Option nur dann zu verwenden, wenn Sie die Benutzererfahrung des Geräts vollständig verstehen. Wenn Ihr Unternehmen ein verwaltetes Google Play-Konto verwendet, können Sie diese Option verwenden, da kein Google-Konto auf den Geräten Ihres Unternehmens vorhanden ist und daher kein werkseitiger Rücksetzschutz auf dem Gerät verfügbar ist.	Android Enterprise Android Management

Es gibt mehrere Möglichkeiten, ein Gerät auf die Werkseinstellungen zurückzusetzen. Der werkseitige Rücksetzschutz reagiert je nach verwendeter Methode unterschiedlich. Weitere Informationen zu vertrauenswürdigen und nicht vertrauenswürdigen Resets finden Sie in KB 56972.

Erstellen eines Profils für werkseitigen Rücksetzschutz

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Verwaltete Geräte > Schutz > Werkseitiger Rücksetzschutz**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie in der Dropdown-Liste **Einstellung für werkseitigen Rücksetzschutz** auf eine der folgenden Optionen:
   - **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. Diese Option wird für Android Enterprise-Geräte (Geschäftlich und persönlich – vollständige Kontrolle und Nur geschäftlicher Bereich) unterstützt.
   - **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. Diese Option wird für Android Enterprise-Geräte (Geschäftlich und persönlich – vollständige Kontrolle und Nur geschäftlicher Bereich) unterstützt.
   - **Google-Kontoanmeldedaten aktivieren und festlegen, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird**: Wählen Sie diese Option aus, um das Google-Konto festzulegen, das nach einem nicht vertrauenswürdigen Zurücksetzen auf die Werkseinstellungen für die Anmeldung am Gerät verwendet werden muss. Wenn Sie diese Option auswählen, können die persönlichen Google-Zugangsdaten des Benutzers nach dem Zurücksetzen auf die Werkseinstellungen nicht mehr verwendet werden. Diese Option

wird für Android Enterprise- und Android Management-Geräte (Geschäftlich und persönlich – vollständige Kontrolle und Nur geschäftlicher Bereich) unterstützt.

Wenn Sie ein verwaltetes Google Play-Konto verwenden möchten, deaktivieren Sie in der IT-Richtlinie, die Benutzern zugewiesen ist, die Option „Wiederherstellen der Werkseinstellungen zulassen“. Dadurch wird die Option zum Wiederherstellen der Werkseinstellungen in den Geräteeinstellungen und die Taste zum Deaktivieren im UEM Client deaktiviert. So wird sichergestellt, dass Benutzer nicht die Option zur nicht vertrauenswürdigen Deaktivierung im UEM Client zur Deaktivierung verwenden, die werkseitigen Rücksetzschutz auf dem Gerät auslöst.

5. Wenn Sie die Option **Anmeldedaten für Google-Konto aktivieren und angeben, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird** ausgewählt haben, klicken Sie auf +, und führen Sie einen der folgenden Schritte aus, um Google-Konten hinzuzufügen (Sie können bis zu 20 hinzufügen):
   - Um die Google-Authentifizierung zu verwenden, klicken Sie auf **Mit Google-Authentifizierung hinzufügen**, und melden Sie sich bei dem Google-Konto an, mit dem Sie sich bei Geräten anmelden möchten, die zurückgesetzt wurden.
   - Um Konten manuell anzugeben, klicken Sie auf **Manuell**. Geben Sie die E-Mail-Adresse und Google-ID an. Um die Google-ID zu erhalten, gehen Sie auf der Website People API für Google-Entwickler wie folgt vor:
     a. Geben Sie für **resourceName** „people/me“ ein.
     b. Geben Sie für **personalFields** „metadata“ ein.
     c. Klicken Sie auf **Ausführen**.
     d. Wählen Sie auf dem Bildschirm **Konto auswählen** ein Konto aus, mit dem Sie das Profil für werkseitigen Rücksetzschutz einrichten möchten.
     e. Klicken Sie auf dem Bildschirm **Google APIs Explorer möchte auf Ihr Google-Konto zugreifen** auf **Zulassen**.
     f. Notieren Sie sich auf der Seite **People ID** die 21-stellige Benutzer-ID.
6. Wenn Sie die Option **Google-Kontoanmeldedaten aktivieren und festlegen, wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird** ausgewählt haben und Ihr Unternehmen über eine Google Workspace- oder Google Cloud-Domäne verfügt, wählen Sie **Google-Konto hinzufügen, das von BlackBerry UEM erstellt wurde**, wenn Sie das geschäftliche Google-Konto des Benutzers in die Liste der Konten aufnehmen möchten, die das Gerät nach einem Zurücksetzen auf die Werkseinstellungen entsperren kann.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.
- Wenn der werkseitige Rücksetzschutz auf dem Gerät ausgelöst wird, funktioniert die Enterprise-Aktivierung bei BlackBerry UEM nicht. Sie müssen zuerst mit dem Out-of-the-Box-Experience von Android den werkseitigen Rücksetzschutz löschen. Siehe Löschen des werkseitigen Rücksetzschutzes von einem Gerät.

Löschen des werkseitigen Rücksetzschutzes von einem Gerät

Wenn der werkseitige Rücksetzschutz auf dem Gerät ausgelöst wird, funktioniert die Enterprise-Aktivierung bei BlackBerry UEM nicht. 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. Wenn 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 die Anmeldedaten für das kommerzielle Google-Konto eingeben, um den BlackBerry UEM Client zu installieren und das Gerät erneut auf UEM zu aktivieren.
   - Auf Samsung-Geräten ohne Zero-Touch-Registrierung oder Samsung Knox Mobile Enrollment: 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 reaktiviert werden.
   - Geräte mit Zero-Touch-Registrierung oder Samsung Knox Mobile Enrollment: 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.

Konfigurieren von Nachweisen für Geräte

Wenn Sie Nachweise aktivieren, sendet BlackBerry UEM Anforderungen zum Testen der Authentizität und Integrität von Geräten. Sie können Nachweise für Samsung Knox-, Android- und Windows 10-Geräte aktivieren.

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

Sie können BlackBerry UEM eine Abfrage mit SafetyNet- oder Google Play Integrity-Nachweis senden lassen, um die Authentizität und Integrität von Android-Geräten und BlackBerry Dynamics-Apps zu testen. Mit SafetyNet und Play Integrity können Sie die Sicherheit und Kompatibilität der Umgebungen bewerten, in denen die Apps Ihres Unternehmens ausgeführt werden. Sie können den SafetyNet- oder Play Integrity-Nachweis neben der bestehenden Root- und Exploit-Erkennung von BlackBerry verwenden. Sie können ein UEM-Konformitätsprofil konfigurieren und zuweisen, um entsprechende Konformitätsaktionen auszuführen, wenn Geräte oder Apps den Nachweis nicht erbringen können.

UEM verwendet die Play Integrity-API mit kompatiblen UEM Client-Versionen, um zusätzlichen Schutz vor Anwendungsmanipulationen zu bieten. Play Integrity ersetzt SafetyNet je nach Migrationsplan, der von Google festgelegt wird. SafetyNet wird weiterhin für ältere Versionen von UEM Client unterstützt. Weitere Informationen zur Migration von SafetyNet finden Sie unter Google Play: Migrieren von der SafetyNet Attestation API.

UEM führt einen SafetyNet- oder Play Integrity-Nachweis unter den folgenden Umständen durch:

- Nach der Geräteaktivierung, wenn BlackBerry UEM Client installiert ist.
- Während und nach der Aktivierung von BlackBerry Dynamics-Apps. Beachten Sie, dass UEM alte Versionen der Apps nicht als vertrauenswürdig behandelt. Um Nachweis-Abfragen zu bestehen, müssen Geräte über die neueste verfügbare Version von BlackBerry Dynamics-Apps verfügen.
- Nach Bedarf mithilfe von REST-APIs.
- Falls der UEM Client aktiviert ist, wenn ein Gerät neu gestartet wird.
- Regelmäßige Nachweisabfragen mit der von Ihnen angegebenen Abfragehäufigkeit.

Der UEM Client ist nicht erforderlich, um den SafetyNet- oder Play Integrity-Nachweis zu aktivieren. Der UEM Client wird nicht in der Liste der BlackBerry Dynamics-Apps angezeigt, die Sie für den SafetyNet- oder Play Integrity-Nachweis konfigurieren können, aber er empfängt und reagiert auf Nachweisabfragen von UEM.

Wenn das Gerät eines Benutzers außer Reichweite ist, ausgeschaltet ist oder eine leere Batterie hat, kann es nicht auf Nachweisabfragen reagieren. Unter diesen Umständen betrachtet UEM das Gerät als nicht konform und führt die Aktionen aus, die Sie im zugewiesenen Konformitätsprofil konfiguriert haben.

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

Bevor Sie beginnen: Die neueste Version der Google Play-Dienste muss auf den Geräten von Benutzern installiert sein.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Nachweis**.
2. Wählen Sie das Kontrollkästchen **Regelmäßige Nachweisabfragen mithilfe von SafetyNet oder Play Integrity aktivieren**.
3. Wenn Sie die Google Compatibility Test Suite aktivieren möchten, wählen Sie das Kontrollkästchen **CTS-Profilanpassung aktivieren**.
4. Geben Sie im Abschnitt **Abfragehäufigkeit** an, wie oft das Gerät eine Nachweisantwort an BlackBerry UEM senden muss. Der Standard- und Mindestwert liegt bei 24 Stunden.

5. Geben Sie im Abschnitt **Übergangsfrist** die Übergangsfrist für Geräte an. Wenn die Übergangsfrist ohne erfolgreiche Nachweisantwort abläuft, wird ein Gerät als nicht richtlinienkonform betrachtet und unterliegt den Aktionen, die Sie im zugewiesenen Konformitätsprofil angeben.
6. Geben Sie im Abschnitt **App-Übergangsfrist** eine Übergangsfrist für BlackBerry Dynamics-Apps an. Wenn die Übergangsfrist ohne erfolgreiche Nachweisantwort abläuft, unterliegen BlackBerry Dynamics-Apps den Aktionen, die Sie im zugewiesenen Konformitätsprofil angeben. Die Übergangsfrist wird pro App erzwungen.
7. Um anzugeben, welche BlackBerry Dynamics-Apps den Nachweisabfragen unterliegen, klicken Sie auf +.
8. Wählen Sie die Apps aus, und klicken Sie auf **Auswählen**.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Aktivieren Sie im Konformitätsprofil, das Geräten zugewiesen ist, die Regel „Fehlgeschlagener SafetyNet- oder Play Integrity-Nachweis“, und konfigurieren Sie die Aktionen, die UEM ausführen soll, wenn es bei Geräten oder BlackBerry Dynamics-Apps fehlgeschlagene Nachweise gab.
- In der Verwaltungskonsole können Sie den Nachweisstatus eines Gerätes in den Gerätedetails anzeigen.

Konfigurieren von Nachweisen für Samsung Knox-Geräte

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

- 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 der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Nachweis**.
2. Aktivieren Sie das Kontrollkästchen **Regelmäßige Nachweisabfragen für KNOX Workspace-Geräte aktivieren**.
3. Geben Sie im Abschnitt **Abfragehäufigkeit** an, wie oft das Gerät eine Nachweisantwort an UEM senden muss.
4. Geben Sie im Abschnitt **Übergangsfrist** die Übergangsfrist für Geräte an. Wenn die Übergangsfrist ohne erfolgreiche Nachweisantwort abläuft, wird ein Gerät als nicht richtlinienkonform betrachtet und unterliegt den Aktionen, die Sie im zugewiesenen Konformitätsprofil angeben.
5. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Aktivieren Sie im Konformitätsprofil, das Geräten zugewiesen ist, die Regel „Gerootetes Betriebssystem oder Fehler bei Knox-Nachweis“, und konfigurieren Sie die Aktionen, die UEM ausführen soll, wenn es bei einem Gerät einen Fehler beim Nachweis gab.

Konfigurieren von Nachweisen für Windows 10-Geräte.

Wenn Sie die Bestätigung aktivieren, sendet BlackBerry UEM Herausforderungen zum Testen der Authentizität und Integrität der Windows 10-Geräte. Beachten Sie, dass die Windows 10-Nachweis-Einstellungen nicht für BlackBerry Desktop (BlackBerry Access + BlackBerry Work) gelten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Nachweis**.
2. Aktivieren Sie das Kontrollkästchen **Regelmäßige Nachweisabfragen für Windows 10-Geräte aktivieren**.
3. Geben Sie im Abschnitt **Abfragehäufigkeit** an, wie oft das Gerät eine Nachweisantwort an UEM senden muss.

4. Geben Sie im Abschnitt **Übergangsfrist** die Übergangsfrist für Geräte an. Wenn die Übergangsfrist ohne erfolgreiche Nachweisantwort abläuft, wird ein Gerät als nicht richtlinienkonform betrachtet und unterliegt den Aktionen, die Sie im zugewiesenen Konformitätsprofil angeben.
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

Wenn Sie fertig sind:

- Konfigurieren Sie im Konformitätsprofil, das Geräten zugewiesen ist, die Regeln „Integritätsnachweis für Windows-Geräte", und konfigurieren Sie die Aktionen, die UEM ausführen soll, wenn es bei einem Gerät einen Fehler beim Nachweis gab.
- In der Verwaltungskonsole können Sie den Nachweisstatus eines Gerätes in den Gerätedetails anzeigen.

Einrichten von Windows-Datenschutz für Windows 10-Geräte

Sie können den Windows-Datenschutz (WIP) für Windows 10-Geräte einrichten, um Folgendes zu erreichen:

- Trennen persönlicher und geschäftlicher Daten auf Geräten.
- Löschen nur geschäftlicher Daten auf Geräten.
- 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 WIP auf Geräten einrichten, legen Sie fest, welche Apps 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. 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.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Schutz > Windows-Datenschutz**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Konfigurieren Sie die entsprechenden Werte für die jeweilige Profileinstellung. Siehe Profileinstellungen für Windows-Datenschutz.
5. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie das Profil Benutzern und Gruppen zu.
- Weisen Sie dem Profil bei Bedarf eine Rangordnung zu.

Profileinstellungen für Windows-Datenschutz

Profileinstellung	Beschreibung
Einstellungen für Windows-Datenschutz	Diese Einstellung legt fest, ob und mit welchen Durchsetzungsmaßnahmen der Windows-Datenschutz aktiviert wird. • Aus: Die Daten sind nicht verschlüsselt, und die Überwachungsprotokollierung ist deaktiviert. • Im Hintergrund: Daten werden verschlüsselt, und alle Versuche, geschützte Daten freizugeben, werden protokolliert. • Außer Kraft setzen: Benutzer werden zur Eingabe aufgefordert, wenn sie versuchen, geschützte Daten freizugeben, und Freigabeversuche werden protokolliert. • Sperren: Daten werden verschlüsselt, Benutzer können geschützte Daten nicht freigeben, und Freigabeversuche werden protokolliert.
Geschützte Domänennamen im Unternehmen	Diese Einstellung legt die geschäftlichen Netzwerkdomänennamen fest, die Ihr Unternehmen für seine Benutzeridentitäten verwendet. Trennen Sie mehrere Domänen mit senkrechten Strichen (|). 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 Zertifikatdatei für die Datenwiederherstellung fest, die Sie zur Wiederherstellung von lokal geschützten Dateien auf einem Gerät verwenden. Die Datei muss ein PEM- oder DER-codiertes Zertifikat mit der Dateierweiterung .der oder .cer sein.
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.
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.

Profileinstellung	Beschreibung
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.
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.

Profileinstellung	Beschreibung

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>`

Profileinstellung	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>`

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.

Profileinstellung	Beschreibung
Überwachungsprotokolle für das Gerät erfassen	Diese Einstellung legt fest, ob Überwachungsprotokolle für das Gerät erfasst werden sollen.

Verschieben von iOS- oder macOS-Geräten in einen gehärteten Kanal

Wenn Sie iOS- oder macOS-Geräte aktivieren, werden die Geräte standardmäßig einem gehärteten Datenkanal zugewiesen. Wenn Sie iOS- oder macOS-Geräte haben, die derzeit keinen gehärteten Kanal verwenden, können Sie eine Liste dieser Geräte exportieren und Maßnahmen ergreifen, um die Geräte in einen gehärteten Kanal zu verschieben. Wenn Sie Geräte in einen gehärteten Kanal verschieben, müssen die Geräte wieder aktiviert werden.

Wenn Sie ein Gerät verschieben, das in Apple-DEP registriert ist, geht die DEP-Registrierungskonfiguration verloren. Gerätebenutzer müssen das Gerät auf die Werkseinstellungen zurücksetzen und mit BlackBerry UEM wieder aktivieren.

Bevor Sie beginnen: Deaktivieren Sie in den App-Einstellungen für die entsprechenden Apps die Option **Die App vom Gerät entfernen, wenn das Gerät von BlackBerry UEM entfernt wird**. Wenn Sie versuchen, Geräte in einen gehärteten Kanal zu verschieben, ohne diese Option zu deaktivieren, wird die App entfernt, und die Registrierung des Geräts in UEM wird möglicherweise aufgehoben. Beachten Sie, dass selbst wenn Sie dieses Kontrollkästchen deaktivieren, Apps beim Verschieben entfernt werden können, wenn die Einstellung nicht an das Gerät gesendet wurde. Weitere Informationen zur Nachverfolgung von Befehlen, die an ein Gerät gesendet werden, finden Sie in KB 102688.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Migration > Gehärteter iOS-Kanal** oder auf **Einstellungen > Migration > Gehärteter macOS-Kanal**.

   Wenn Sie keine dieser Menüoptionen sehen, gibt es in Ihrer UEM-Umgebung keine iOS- oder macOS-Geräte, die in einen gehärteten Kanal verschoben werden müssen.
2. Klicken Sie auf **Exportieren**, um eine Liste von Geräten zu herunterzuladen, die derzeit keinen gehärteten Kanal verwenden.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Verschieben mehrerer iOS-Geräte in einen gehärteten Kanal.	Klicken Sie auf **Durchsuchen**, navigieren Sie zur Datei, die Sie in Schritt 2 heruntergeladen haben, und wählen Sie sie aus. Geräte, die zu freigegebenen Gerätegruppen gehören, werden in der Datei nur zu Informationszwecken aufgeführt und mit dieser Methode nicht in einen gehärteten Kanal verschoben. Für alle Geräte, die zu freigegebenen Gerätegruppen gehören, muss der Benutzer das Gerät auf Werkseinstellungen zurücksetzen und mit UEM wieder aktivieren. Mit dieser Methode können maximal 1000 Einträge gleichzeitig verarbeitet werden. Wenn die heruntergeladene Datei mehr als 1000 Einträge enthält, teilen Sie sie in separate Dateien auf, die jeweils maximal 1000 Einträge enthalten.
Verschieben eines bestimmten iOS-Geräts in einen gehärteten Kanal.	**a.** Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**. **b.** Suchen Sie nach dem iOS-Gerät, und klicken Sie es an. **c.** Klicken Sie auf der Registerkarte „Gerät“ auf **Auf gehärteten iOS-Kanal migrieren**. **d.** Klicken Sie auf **Submit**.
Verschieben Sie macOS-Geräte in einen gehärteten Kanal.	Kontaktieren Sie Gerätebenutzer, und weisen Sie sie an, ihr Gerät mit UEM Self-Service wieder zu aktivieren.

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada