



BlackBerry UEM

Verwaltung

Verwalten von Administratoren, Benutzern und Gruppen

12.19

Contents

Verwalten von BlackBerry UEM-Administratoren, -Benutzern und -Gruppen.....	5
Konfigurieren der Konsolenanmeldeoptionen.....	6
Festlegen der Mindestkomplexität des Kennworts für lokale Administratoren.....	6
Erstellen eines Anmeldungshinweises für die Konsolen.....	7
Einstellen des Grenzwerts für das Sitzungs-Timeout.....	7
Einmalige Anmeldung für BlackBerry UEM einrichten.....	8
Konfigurieren der zertifikatbasierten Konsolen-Authentifizierung.....	9
Erstellen und Verwalten von Administratorregeln.....	10
Berechtigungen für vorkonfigurierte Administratorrollen.....	10
Erstellen einer benutzerdefinierten Administratorrolle.....	37
Verwalten von Administratorrollen.....	38
Erstellen eines Administrators.....	39
Erstellen und Verwalten von Benutzerkonten.....	40
Erstellen eines Benutzerkontos.....	40
Erstellen von Benutzerkonten aus einer .csv-Datei.....	42
Hinzufügen von Benutzerkonten zu UEM mithilfe einer .csv-Datei.....	43
Aktivieren von Diensten für einen Benutzer.....	44
Hinzufügen von Benutzern zu Benutzergruppen.....	44
Verwalten von Benutzerkonten.....	45
Kommunikation an Benutzer senden.....	46
Erstellen und Verwalten von Benutzergruppen.....	47
Erstellen einer per Verzeichnis verknüpften Gruppe.....	47
Hinzufügen einer Unternehmensverzeichnisgruppe zu einer vorhandenen per Verzeichnis verknüpften Gruppe.....	49
Erstellen einer lokalen Gruppe.....	49
Hinzufügen von verschachtelten Gruppen zu einer Benutzergruppe.....	50
Verwalten einer Benutzergruppe.....	51
Erstellen und Verwalten von Gerätegruppen.....	52
Erstellen einer Gerätegruppe.....	52
Parameter für Gerätegruppen.....	53
Verwalten einer Gerätegruppe.....	54
Freigegebene Gerätegruppen erstellen und bearbeiten.....	56

Freigegebene Gerätegruppe erstellen.....	56
Aktivieren eines freigegebenen Geräts.....	57
Verwalten einer freigegebenen Gerätegruppe.....	57
Erstellen und Verwalten öffentlicher Gerätegruppen.....	60
Erstellen einer öffentlichen Gerätegruppe.....	60
Aktivieren eines öffentlichen Geräts.....	61
Verwalten einer öffentlichen Gerätegruppe.....	61
Erstellen und Verwalten von Gruppen gemeinsam genutzter iPad s.....	62
Erstellen einer Gruppe gemeinsam genutzter iPad s.....	62
Erstellen eines Profils für ein gemeinsam genutztes iPad.....	62
Aktivieren eines gemeinsam genutzten iPad-Geräts.....	63
Verwalten einer Gruppe gemeinsam genutzter iPad s.....	63
Verwalten von Chrome OS-Geräten in BlackBerry UEM.....	65
Chrome OS-Geräte verwalten.....	65
Einrichtung der BlackBerry UEM Self-Service.....	67
Verwalten von Benutzerrollen für BlackBerry UEM Self-Service.....	68
BlackBerry UEM Self-Service-Funktionen.....	68
Erstellen einer Benutzerrolle für UEM Self-Service.....	69
Anpassen der Benutzerliste.....	70
Rechtliche Hinweise.....	72

Verwalten von BlackBerry UEM-Administratoren, -Benutzern und -Gruppen

Diese Anleitung enthält Anweisungen und Details zum Erstellen und Konfigurieren von Administratorkonten, Benutzerkonten und Gruppen zur Verwaltung der BlackBerry UEM-Unternehmensumgebung.

Aufgabe	Beschreibung
Konfigurieren der Anmeldeoptionen für die Verwaltungskonsole.	Konfigurieren Sie, wie sich Administratoren und Benutzer bei UEM-Konsolen authentifizieren, einschließlich Komplexität von Kennwörtern, Anmeldungshinweisen, Sitzungszeitüberschreitungs-Grenzwerten und Optionen wie verzeichnisbasierte Authentifizierung und Single Sign-On.
Erstellen und Verwalten von Administratorrollen.	Verwenden Sie vorkonfigurierte Administratorrollen, oder erstellen Sie benutzerdefinierte Rollen, um den Grad der Kontrolle und Berechtigungen zu konfigurieren, die Administratoren in der Verwaltungskonsole haben.
Erstellen eines Administrators.	Erstellen Sie Administratorbenutzer, um die UEM-Umgebung Ihres Unternehmens zu verwalten.
Erstellen und Verwalten von Benutzerkonten.	Erstellen Sie Benutzerkonten direkt in UEM, oder erstellen Sie Benutzerkonten aus dem Unternehmensverzeichnis Ihrer Organisation.
Erstellen und Verwalten von Benutzergruppen.	Erstellen Sie Benutzergruppen, um Einstellungen und Konfigurationen auf mehrere Benutzer anzuwenden.
Erstellen und Verwalten von Gerätegruppen.	Erstellen Sie Gerätegruppen, um Einstellungen und Konfigurationen auf bestimmte Gerätetypen anzuwenden.
Erstellen und Verwalten von freigegebenen Gerätegruppen.	Erstellen Sie freigegebene Gerätegruppen, damit mehrere Benutzer ein iOS-Gerät gemeinsam nutzen können.
Erstellen und Verwalten von öffentlichen Gerätegruppen.	Erstellen Sie öffentliche Gerätegruppen zur Verwaltung von iOS- oder Android Enterprise-Geräten, die einen bestimmten Zweck erfüllen und für eine bestimmte App-Gruppe gesperrt sind.
Erstellen und Verwalten von Gruppen gemeinsam genutzter iPads.	Erstellen Sie Gruppen gemeinsam genutzter iPads, damit sich mehrere Benutzer bei einem gemeinsam genutzten iPad anmelden und dieses verwenden können.
Verwalten von Chrome OS-Geräten.	Verwenden Sie UEM zum Ausführen von Verwaltungsaktionen für Chrome OS-Geräte.
Einrichtung der BlackBerry UEM Self-Service.	Gewähren Sie Benutzern Zugriff auf UEM Self-Service, um Self-Service-Geräteverwaltungsaufgaben auszuführen.
Erstellen von Benutzerrollen für UEM Self-Service.	Verwenden Sie Rollen, um Endbenutzer-Berechtigungen für UEM Self-Service zu verwalten.
Anpassen der Benutzerliste.	Ändern Sie die Liste der Benutzerkonten in der Verwaltungskonsole nach Ihren Anforderungen.

Konfigurieren der Konsolenanmeldeoptionen

Sie können konfigurieren, wie sich Administratoren und Benutzer bei den BlackBerry UEM-Konsolen authentifizieren, einschließlich der erforderlichen Kennwortkomplexität, der Anmeldungshinweise und der Grenzwerte für Sitzungszeitüberschreitungen.

Sie können Administratoren und Benutzern die Anmeldung mit den folgenden Authentifizierungsmethoden ermöglichen:

Authentifizierungsoption	Beschreibung
Lokale kennwortbasierte Authentifizierung	Lokale Administratoren und Benutzer können sich mit einem Benutzernamen und Kennwort authentifizieren.
Verzeichnisbasierte Authentifizierung	Wenn Sie BlackBerry UEM mit Ihrem Unternehmensverzeichnis verbinden, können sich Administratoren und Benutzer mit ihren Verzeichnisanmeldedaten anmelden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihren Unternehmensverzeichnissen in der Dokumentation zur Konfiguration.
Einmalige Anmeldung	Wenn Sie in einer lokalen Umgebung eine Verbindung zwischen UEM und Microsoft Active Directory herstellen, können Sie die Authentifizierung per einmaliger Anmeldung konfigurieren, damit Administratoren bzw. Benutzer die Webseite für die Anmeldung umgehen und direkt auf die Verwaltungskonsole bzw. BlackBerry UEM Self-Service zugreifen können. Für die Anmeldung ist kein Kennwort oder Zertifikat erforderlich. Siehe Einmalige Anmeldung für BlackBerry UEM einrichten . Diese Funktion wird von UEM Cloud nicht unterstützt.
Zertifikatsbasierte Authentifizierung	Sie können eine zertifikatbasierte Authentifizierung einrichten, damit sich Administratoren und Benutzer mit einem Authentifizierungszertifikat anmelden können. Siehe Konfigurieren der zertifikatbasierten Konsolen-Authentifizierung . Diese Funktion wird von UEM Cloud nicht unterstützt.
BlackBerry 2FA-Authentifizierung	Sie können eine BlackBerry 2FA-Authentifizierung einrichten, damit sich Administratoren und Benutzer mit der Zwei-Faktor-Authentifizierung anmelden können. Weitere Informationen finden Sie in KB 73371 . Diese Funktion wird in lokalen Umgebungen nicht unterstützt.
BlackBerry Online Account-Authentifizierung	Sie können die BlackBerry Online Account-Authentifizierung so einrichten, dass Administratoren sich mit ihren BlackBerry Online Account-Anmeldeinformationen anmelden können. Diese Funktion wird in lokalen Umgebungen nicht unterstützt.


Festlegen der Mindestkomplexität des Kennworts für lokale Administratoren

Sie können die Mindestlänge und Komplexität von Kennwörtern für lokale Administratorkonten festlegen. Die Einstellung wird wirksam, wenn Administratoren ihr Kontokennwort ändern.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Konsole**.
2. Legen Sie im Feld **Mindestzahl von Zeichen** fest, wie viele Zeichen ein Konsolenkennwort mindestens aufweisen muss.
3. Wählen Sie im Feld **Mindestkomplexität des Kennworts** aus, welche Komplexität das Konsolenkennwort aufweisen muss.
4. Klicken Sie auf **Speichern**.

Erstellen eines Anmeldungshinweises für die Konsolen

Sie können einen Anmeldungshinweis für Administratoren oder Benutzer in einer lokalen Umgebung erstellen, der angezeigt wird, wenn diese sich bei der BlackBerry UEM-Verwaltungskonsole oder dem BlackBerry UEM Self-Service anmelden. Der Hinweis informiert die Administratoren oder Benutzer über die an die Verwendung der Konsolen geknüpften Geschäftsbedingungen, die diese akzeptieren müssen. Diese Funktion wird für UEM Cloud nicht unterstützt.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Anmeldungshinweise**.
2. Klicken Sie auf .
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Konfigurieren des Anmeldungshinweises für die UEM-Verwaltungskonsole.	<ol style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen Anmeldungshinweis für die Verwaltungskonsole aktivieren. b. Geben Sie die Daten ein, die Administratoren angezeigt werden sollen, wenn sie sich anmelden.
Konfigurieren eines Anmeldungshinweises für UEM Self-Service.	<ol style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen Anmeldungshinweis für die Selbstbedienungskonsole aktivieren. b. Geben Sie die Daten ein, die den Benutzern angezeigt werden sollen, wenn sie sich anmelden.

4. Klicken Sie auf **Speichern**.

Einstellen des Grenzwerts für das Sitzungs-Timeout

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Allgemeine Einstellungen > Konsole**.
2. Geben Sie im Feld **Sitzungs-Timeout** die Zeitspanne in Minuten an, bis die Sitzung wegen Timeout abgebrochen und der Benutzer abgemeldet wird.
3. Geben Sie im Feld **Warnung zum Sitzungs-Timeout** die Zeitspanne in Minuten vor der Abmeldung eines Benutzers an, bis die Warnung zum Sitzungs-Timeout angezeigt wird.
4. Klicken Sie auf **Speichern**.

Einmalige Anmeldung für BlackBerry UEM einrichten

Wenn Sie eine Verbindung zwischen BlackBerry UEM und Microsoft Active Directory herstellen, können Sie die Authentifizierung per einmaliger Anmeldung konfigurieren, damit Administratoren bzw. Benutzer die Webseite für die Anmeldung umgehen und direkt auf die Verwaltungskonsole bzw. BlackBerry UEM Self-Service zugreifen können. Wenn Administratoren oder Benutzer sich bei Windows anmelden, verwendet der Browser ihre Anmeldeinformationen zur automatischen Authentifizierung bei UEM. Windows-Anmeldeinformationen können Active Directory-Anmeldeinformationen oder abgeleitete Anmeldeinformationen (z. B. von CAC-Lesern oder digitalen Tokens) umfassen.

Diese Funktion wird von UEM Cloud nicht unterstützt.

Bevor Sie beginnen:

- Führen Sie die folgenden Schritte aus, um die eingeschränkte Delegation für das Active Directory-Konto zu konfigurieren, das von UEM für die Verzeichnisverbindung verwendet wird:
 1. Fügen Sie dem Windows Server-Konto mithilfe von UEM ADSI Edit oder dem Befehlszeilentool „setspn“ die folgenden SPN für Active Directory hinzu:
HTTP/<host_FQDN_or_pool_name> (z. B. HTTP/domäne123.beispiel.com)
BASPLUGIN111/<host_FQDN_or_pool_name> (z. B. BASPLUGIN111/domäne123.beispiel.com)
 2. Aktivieren Sie in den Microsoft Active Directory-Kontoeigenschaften von Microsoft Active Directory Users and Computers auf der Registerkarte **Delegation** die Option **Benutzer nur bei Delegierungen angegebener Dienste vertrauen** und **Nur Kerberos verwenden**.
 3. Fügen Sie zur Liste der Dienste die SPN hinzu.
- Wenn Sie die einmalige Anmeldung für mehrere Active Directory-Verbindungen aktivieren, stellen Sie sicher, dass es keine Vertrauensbeziehungen zwischen den Active Directory-Gesamtstrukturen gibt.
 1. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
 2. Klicken Sie im Abschnitt **Konfigurierte Verzeichnisverbindungen** auf eine Active Directory-Verbindung.
 3. Markieren Sie auf der Registerkarte **Authentifizierung** das Kontrollkästchen **Windows Single Sign-On aktivieren**.
 4. Klicken Sie auf **Speichern**.
 5. Klicken Sie erneut auf **Speichern**.
 6. Klicken Sie auf **Schließen**.

Wenn Sie fertig sind:

- Starten Sie die UEM-Dienste auf jedem Computer, der eine UEM-Instanz hostet, neu.
 - Weisen Sie Administratoren und Benutzer an, die folgenden URLs zu verwenden:
 - Verwaltungskonsole: https://<host_FQDN_or_pool_name>:<port>/admin
 - UEM Self-Service: https://<host_FQDN_or_pool_name>:<port>/mydevice
- Die Authentifizierung per einmaliger Anmeldung hat Vorrang vor anderen Authentifizierungsmethoden. Wenn die Sicherheitsstandards Ihres Unternehmens erfordern, dass Administratoren oder Benutzer eine andere Authentifizierungsmethode verwenden, kann die Single Sign-On-Methode umgangen werden, indem Sie an das Ende der oben genannten URLs „?sso=n“ anhängen.
- Weisen Sie Administratoren und UEM Self-Service-Benutzer an, ihre Browser für die einmalige Anmeldung an UEM zu konfigurieren:
 - Microsoft Edge: Die URLs von Verwaltungskonsole und UEM Self-Service müssen der lokalen Intranetzzone zugewiesen sein. Aktivieren Sie die integrierte Windows-Authentifizierung.

- Mozilla Firefox: Fügen Sie in der Liste „about:config“ „https://, <host_FQDN_or_pool_name>“ zur Einstellung „network.negotiate-auth.trusted-uris“ hinzu.
- Google Chrome: Die URLs von Verwaltungskonsolle und UEM Self-Service müssen der lokalen Intranetzzone zugewiesen sein.

Konfigurieren der zertifikatbasierten Konsolen-Authentifizierung

In einer lokalen BlackBerry UEM-Umgebung können Sie eine zertifikatbasierte Authentifizierung einrichten, damit sich Administratoren mit einem Authentifizierungszertifikat anmelden können. UEM überprüft Zertifikate gegen den Aussteller, verifiziert die Gültigkeit des Zertifikats mit den OCSP- oder CRL-Einstellungen und stellt sicher, dass das Zertifikat mit einem Benutzer in der UEM-Datenbank übereinstimmt. Diese Funktion wird für UEM Cloud nicht unterstützt.

Bevor Sie beginnen: Holen Sie sich Kopien der Zertifizierungsstellenzertifikate, die die Client-Zertifikate Ihrer Administratoren und Benutzer im CER- oder DER-Format verbreiten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Einstellungen > Allgemeine Einstellungen > Zertifikatsbasierte Konsolen-Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen **Zertifikatsbasierte Authentifizierung aktivieren**.
3. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu der Zertifizierungsstellen-Zertifikatdatei.
UEM vertraut allen Zertifikaten, die von dieser Zertifizierungsstelle ausgestellt wurden. Wiederholen Sie diesen Schritt, um weitere Zertifikate hochzuladen.
4. Damit UEM überprüfen muss, ob der Benutzerprinzipalname im Zertifikat mit einem Benutzer in der UEM-Datenbank übereinstimmt, aktivieren Sie das Kontrollkästchen **Auf Benutzerprinzipalname für SAN überprüfen**.
Wenn der Benutzerprinzipalname im Zertifikat mit einem bekannten Benutzer übereinstimmt, gewährt UEM entsprechend den Berechtigungen des Benutzers Zugriff.
5. Damit UEM prüfen muss, ob die E-Mail-Adresse des Benutzers im Zertifikat mit der E-Mail-Adresse eines Benutzers in der UEM-Datenbank übereinstimmt, wählen Sie **Auf E-Mail-Adresse überprüfen**.
Wenn die Benutzer-E-Mail-Adresse im Zertifikat mit einem bekannten Benutzer übereinstimmt, gewährt UEM entsprechend den Berechtigungen des Benutzers Zugriff. Wenn Sie sowohl **Auf Benutzerprinzipalname für SAN überprüfen** als auch **Auf E-Mail-Adresse überprüfen** auswählen, überprüft UEM den Prinzipalnamen vor der E-Mail-Adresse und gewährt Zugriff, wenn der Prinzipalname übereinstimmt. Wenn keine der Prüfungen eine Übereinstimmung zwischen dem Zertifikat und einem bekannten Benutzer ergibt, verweigert UEM den Zugriff.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Wenn Benutzer über Mozilla Firefox auf UEM zugreifen, muss der Benutzer sein Clientzertifikat zum Firefox-Zertifikatspeicher hinzufügen, um sich über die zertifikatbasierte Authentifizierung bei UEM zu authentifizieren.

Erstellen und Verwalten von Administratorregeln

Sie können Administratoren vorkonfigurierte Rollen zuweisen oder benutzerdefinierte Rollen erstellen, die den Anforderungen Ihres Unternehmens entsprechen. Sie müssen ein Sicherheitsadministrator sein, um benutzerdefinierte Rollen erstellen, Informationen zu einer Rolle anzeigen, Rolleneinstellungen ändern, Rollen eine Rangordnung zuweisen und Rollen löschen zu können.

Berechtigungen für vorkonfigurierte Administratorrollen

BlackBerry UEM schließt vier vorkonfigurierte Rollen für Administratoren ein. Die Rolle des Sicherheitsadministrators verfügt über volle Berechtigungen, einschließlich der Erstellung und Verwaltung von Rollen und Administratoren. Sie können die Rolle nicht bearbeiten oder löschen. Mindestens einem Administrator muss die Rolle „Sicherheitsadministrator“ zugewiesen sein. Die Rolle „Enterprise-Administrator“ (alle Berechtigungen außer die für die Erstellung und Verwaltung von Rollen und Administratoren), die Rolle „Senior Helpdesk“ (Berechtigungen zur Durchführung fortgeschrittener administrativer Aufgaben) und die Rolle „Junior Helpdesk“ (Berechtigungen zur Durchführung grundlegender administrativer Aufgaben) können bearbeitet oder gelöscht werden. In den folgenden Tabellen werden die Berechtigungen aufgeführt, die für jede vorkonfigurierte Rolle standardmäßig eingeschaltet werden.

Einige Berechtigungen werden nur in benutzerdefinierten Rollen unterstützt.

Rollen und Administratoren

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Rollen anzeigen	✓	NA	NA	NA
Erstellen und Bearbeiten von Rollen	✓	NA	NA	NA
Löschen von Rollen	✓	NA	NA	NA
Zuweisen eines Rangs zu Rollen	✓	NA	NA	NA
Administratoren erstellen	✓	NA	NA	NA
Administratoren löschen	✓	NA	NA	NA
Nicht-administrative Attribute von Administratoren bearbeiten	✓	NA	NA	NA
Kennwort für andere Administratoren ändern	✓	NA	NA	NA

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Rollenmitgliedschaft für Administratoren ändern	✓	NA	NA	NA

Verzeichniszugriff

Sie haben die Möglichkeit, anzugeben, welche Unternehmensverzeichnisse der Administrator durchsuchen kann.

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Alle Firmenverzeichnisse	✓	✓	✓	✓
Nur ausgewählte Unternehmensverzeichni				

Gruppenverwaltung

Sie haben die Möglichkeit, anzugeben, welche Gruppen der Administrator verwalten kann. Um Benutzer zu verwalten, die keiner Gruppe angehören, müssen Administratoren über die Berechtigung verfügen, alle Gruppen und Benutzer zu verwalten.

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Alle Gruppen und Benutzer	✓	✓	✓	✓
Ausgewählte Gruppen				

Benutzer und Geräte

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Benutzer und aktivierte Geräte anzeigen	✓	✓	✓	✓
Benutzer erstellen	✓	✓	✓	
Benutzer bearbeiten	✓	✓	✓	✓
Benutzerrollen zuweisen	✓	✓	✓	✓

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Benutzer löschen	✓	✓	✓	
Benutzerliste exportieren	✓	✓		
Ein Aktivierungskennwort generieren und E-Mail senden	✓	✓	✓	✓
Aktivierungskennwörter generieren und Aktivierungsnachrichten per E-Mail an mehrere Benutzer senden	✓	✓	✓	
Ein Aktivierungskennwort festlegen	✓	✓	✓	✓
Legen Sie mehrere Aktivierungskennwörter mit eindeutigen Aktivierungsprofilen für einen Benutzer fest	✓	✓		
Legen Sie fest, ob Aktivierungskennwörter nach der Aktivierung des ersten Geräts ablaufen	✓	✓		
QR-Codes und Zugriffsschlüssel für Benutzeraktivierung anzeigen	✓	✓		
Kontokennwort festlegen	✓	✓	✓	✓
Mehrere Kontokennwörter ändern	✓	✓	✓	
BlackBerry 2FA-Vorauthentifizierung einrichten	✓	✓		
Geräte verwalten	✓	✓	✓	✓

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Geschäftlichen Bereich aktivieren	✓	✓	✓	✓
Geschäftlichen Bereich deaktivieren	✓	✓	✓	✓
Geschäftlichen Bereich sperren	✓	✓	✓	✓
Kennwort für geschäftlichen Bereich zurücksetzen	✓	✓	✓	✓
Gerätekenwort festlegen	✓	✓	✓	✓
Gerät sperren und Nachricht einrichten	✓	✓	✓	✓
Gerät entsperren und Kennwort löschen	✓	✓	✓	✓
Nur geschäftliche Daten löschen	✓	✓	✓	✓
Nur geschäftliche Daten von mehreren Geräten löschen	✓			
Alle Gerätedaten löschen	✓	✓	✓	✓
Alle Gerätedaten von mehreren Geräten löschen	✓			
Gerät löschen	✓	✓		
Mehrere Geräte löschen	✓			
Geschäftliches Kennwort festlegen und sperren	✓	✓	✓	✓
Geräteprotokolle abrufen	✓	✓	✓	

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Aktivierungssperre aktivieren	✓	✓	✓	✓
Aktivierungssperre deaktivieren	✓	✓	✓	✓
Verloren-Modus	✓	✓	✓	✓
Verloren-Modus aktivieren	✓	✓	✓	✓
Deaktivieren des Verloren-Modus	✓	✓	✓	✓
Standort des Geräts bestimmen	✓	✓	✓	✓
Gerät anmelden	✓	✓	✓	
Gerät neu starten	✓	✓	✓	✓
iOS-Software aktualisieren	✓	✓	✓	✓
iOS-Software auf mehreren Geräten aktualisieren	✓			
Gerät abschalten	✓	✓	✓	✓
Details zum Gerätestandort anzeigen	✓	✓	✓	
Verlauf des Gerätestandorts anzeigen	✓	✓		
Informationen zu Exchange Gatekeeping anzeigen	✓	✓		
Apple DEP-Geräteinformationen anzeigen	✓	✓	✓	✓
Registrierungskonfigurationen zuweisen	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Token für Einmalkennwort anzeigen	✓	✓	✓	✓
Token für Einmalkennwort zuweisen	✓	✓		
E-Mail an Benutzer senden	✓	✓	✓	
Umgehungsverlauf der Aktivierungssperre anzeigen	✓	✓	✓	
Verwalten von BlackBerry Dynamics-Apps	✓	✓	✓	✓
App sperren	✓	✓	✓	
App entsperren	✓	✓	✓	✓
App-Daten löschen	✓	✓	✓	✓
App-Protokollierung steuern	✓	✓	✓	
Verwalten von Intune-Apps	✓	✓	✓	

Dediziertes Gerät

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Einstellungen für freigegebene Gerätegruppen anzeigen	✓	✓		
Freigegebene Gerätegruppen erstellen und bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Freigegebene Gerätegruppen löschen	✓	✓		
Einstellungen für öffentliche Gerätegruppen anzeigen	✓	✓		
Öffentliche Gerätegruppen erstellen und bearbeiten	✓	✓		
Öffentliche Gerätegruppen löschen	✓	✓		

Gruppen

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Gruppeneinstellungen anzeigen	✓	✓	✓	✓
Benutzergruppen erstellen und bearbeiten	✓	✓	✓	
Benutzerrollen zuweisen	✓	✓	✓	
Benutzer zu Benutzergruppen hinzufügen oder aus ihnen entfernen	✓	✓	✓	
Benutzergruppen löschen	✓	✓		
Gerätegruppen erstellen und bearbeiten	✓	✓	✓	
Gerätegruppen löschen	✓	✓		

Richtlinien und Profile

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
IT-Richtlinien anzeigen	✓	✓	✓	✓
IT-Richtlinien erstellen und bearbeiten	✓	✓		
IT-Richtlinien löschen	✓	✓		
E-Mail-Profile anzeigen	✓	✓	✓	✓
E-Mail-Profile erstellen und bearbeiten	✓	✓		
E-Mail-Profile löschen	✓	✓		
IMAP/POP3-E-Mail-Profile anzeigen	✓	✓	✓	✓
IMAP/POP3-E-Mail-Profile erstellen und bearbeiten	✓	✓		
IMAP/POP3-E-Mail-Profile löschen	✓	✓		
Profile anzeigen, die Enterprise-Konnektivität bereitstellen	✓	✓	✓	✓
Profile, die Enterprise-Konnektivität bereitstellen, erstellen und bearbeiten	✓	✓		
Profile löschen, die Enterprise-Konnektivität bereitstellen	✓	✓		
Profile für Geräte-SR-Anforderungen anzeigen	✓	✓	✓	✓
Profile für Gerätedienstanforderung erstellen oder bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Profile für Geräte-SR-Anforderungen löschen	✓	✓		
Aktivierungsprofile anzeigen	✓	✓	✓	✓
Aktivierungsprofile erstellen und bearbeiten	✓	✓		
Aktivierungsprofile löschen	✓	✓		
Wi-Fi-Profile anzeigen	✓	✓	✓	✓
Wi-Fi-Profile erstellen und bearbeiten	✓	✓		
Wi-Fi-Profile löschen	✓	✓		
VPN-Profile anzeigen	✓	✓	✓	✓
VPN-Profile erstellen und bearbeiten	✓	✓		
VPN-Profile löschen	✓	✓		
Profile für die Kompatibilitätsprüfung anzeigen	✓	✓	✓	✓
Profile für die Kompatibilitätsprüfung erstellen und bearbeiten	✓	✓		
Profile für die Kompatibilitätsprüfung löschen	✓	✓		
Geräteprofile anzeigen	✓	✓	✓	✓
Geräteprofile erstellen und bearbeiten	✓			
Geräteprofile löschen	✓	✓		
Proxy-Profile anzeigen	✓	✓	✓	✓

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Proxy-Profilen erstellen und bearbeiten	✓	✓		
Proxy-Profilen löschen	✓	✓		
Webinhaltsfilter-Profilen anzeigen	✓	✓	✓	✓
Webinhaltsfilter-Profilen erstellen und bearbeiten	✓	✓		
Webinhaltsfilter-Profilen löschen	✓	✓		
FileVault-Profilen anzeigen	✓	✓	✓	✓
FileVault-Profilen erstellen und bearbeiten	✓	✓		
FileVault-Profilen löschen	✓	✓		
Standortbestimmungsprofilen anzeigen	✓	✓	✓	✓
Standortbestimmungsprofilen erstellen und bearbeiten	✓	✓		
Standortbestimmungsprofilen löschen	✓	✓		
App-Sperrmodus-Profilen anzeigen	✓	✓	✓	✓
App-Sperrmodus-Profilen erstellen und bearbeiten	✓	✓		
App-Sperrmodus-Profilen löschen	✓	✓		
Profile für die einmalige Anmeldung anzeigen	✓	✓	✓	✓

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Profile für die einmalige Anmeldung erstellen und bearbeiten	✓	✓		
Profile für die einmalige Anmeldung löschen	✓	✓		
Profile für Zertifizierungsstellenzertifikat anzeigen	✓	✓	✓	✓
Profile für Zertifizierungsstellenzert erstellen und bearbeiten	✓	✓		
Profile für Zertifizierungsstellenzertifikat löschen	✓	✓		
Profile für freigegebenes Zertifikat anzeigen	✓	✓	✓	✓
Profile für freigegebenes Zertifikat erstellen und bearbeiten	✓	✓		
Profile für freigegebenes Zertifikat löschen	✓	✓		
SCEP-Profile anzeigen	✓	✓	✓	✓
SCEP-Profile erstellen und bearbeiten	✓	✓		
SCEP-Profile löschen	✓	✓		
OCSP-Profile anzeigen	✓	✓	✓	✓
OCSP-Profile erstellen und bearbeiten	✓	✓		
OCSP-Profile löschen	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Zertifikatabrufprofile anzeigen	✓	✓	✓	✓
Zertifikatabrufprofile erstellen und bearbeiten	✓	✓		
Zertifikatabrufprofile löschen	✓	✓		
CRL-Profile anzeigen	✓	✓	✓	✓
CRL-Profile erstellen und bearbeiten	✓	✓		
CRL-Profile löschen	✓	✓		
Profile für verwaltete Domänen anzeigen	✓	✓	✓	✓
Profile für verwaltete Domänen erstellen und bearbeiten	✓	✓		
Profile für verwaltete Domänen löschen	✓	✓		
Profile mit Benutzeranmeldeinforma anzeigen	✓	✓	✓	✓
Profile mit Benutzeranmeldeinformationen erstellen und bearbeiten	✓	✓		
Profile mit Benutzeranmeldeinforma löschen	✓	✓		
Benutzerdefinierte Payload-Profile anzeigen	✓	✓	✓	✓
Benutzerdefinierte Payload-Profile erstellen und bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Benutzerdefinierte Payload-Profilen löschen	✓	✓		
Benutzern IT-Richtlinien und Profile zuweisen	✓	✓	✓	✓
Benutzergruppen IT-Richtlinien und Profile zuweisen	✓	✓	✓	✓
Gerätegruppen IT-Richtlinien und Profile zuweisen	✓	✓	✓	✓
Freigegebenen Gerätegruppen IT-Richtlinien und Profile zuweisen	✓	✓		
Öffentlichen Gerätegruppen IT-Richtlinien und Profile zuweisen	✓	✓		
IT-Richtlinien und Profilen einen Rang zuweisen	✓	✓		
CardDAV-Profilen anzeigen	✓	✓	✓	✓
CardDAV-Profilen erstellen und bearbeiten	✓	✓		
CardDAV-Profilen löschen	✓	✓		
CalDAV-Profilen anzeigen	✓	✓	✓	✓
CalDAV-Profilen erstellen und bearbeiten	✓	✓		
CalDAV-Profilen löschen	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
AirPrint-Profilen anzeigen	✓	✓	✓	✓
AirPrint-Profilen erstellen und bearbeiten	✓	✓		
AirPrint-Profilen löschen	✓	✓		
Netzwerknutzungsprofile anzeigen	✓	✓	✓	✓
Netzwerknutzungsprofile erstellen und bearbeiten	✓	✓		
Netzwerknutzungsprofile löschen	✓	✓		
AirPlay-Profilen anzeigen	✓	✓	✓	✓
AirPlay-Profilen erstellen und bearbeiten	✓	✓		
AirPlay-Profilen löschen	✓	✓		
Enterprise Management Agent-Profilen anzeigen	✓	✓	✓	✓
Enterprise Management Agent-Profilen erstellen und bearbeiten	✓	✓		
Enterprise Management Agent-Profilen löschen	✓	✓		
BlackBerry Dynamics-Konformitätsprofile anzeigen	✓	✓	✓	✓
BlackBerry Dynamics-Konformitätsprofile löschen	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
BlackBerry Dynamics-Profilen anzeigen	✓	✓	✓	✓
BlackBerry Dynamics-Profilen erstellen und bearbeiten	✓	✓		
BlackBerry Dynamics-Profilen löschen	✓	✓		
BlackBerry Dynamics-Konnektivitätsprofilen anzeigen	✓	✓	✓	✓
BlackBerry Dynamics-Konnektivitätsprofilen erstellen und bearbeiten	✓	✓		
BlackBerry Dynamics-Konnektivitätsprofilen löschen	✓	✓		
Nicht-stören-Profilen anzeigen	✓	✓	✓	✓
Nicht-stören-Profilen erstellen und bearbeiten	✓	✓		
Nicht-stören-Profilen löschen	✓	✓		
BlackBerry 2FA-Profilen anzeigen	✓	✓	✓	✓
BlackBerry 2FA-Profilen erstellen und bearbeiten	✓	✓		
BlackBerry 2FA-Profilen löschen	✓	✓		
Windows-Datenschutzprofilen anzeigen	✓	✓	✓	✓

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Windows-Datenschutzprofile erstellen und bearbeiten	✓	✓		
Windows-Datenschutzprofile löschen	✓	✓		
Per-App-Benachrichtigungsprofile anzeigen	✓	✓	✓	✓
Per-App-Benachrichtigungsprofile erstellen und bearbeiten	✓	✓		
Per-App-Benachrichtigungsprofile löschen	✓	✓		
Gatekeeping-Profile anzeigen	✓	✓	✓	✓
Gatekeeping-Profile erstellen und bearbeiten	✓	✓		
Gatekeeping-Profile l \u00f6schen	✓	✓		
Sicherheitsprofile für Microsoft Intune-App anzeigen	✓	✓	✓	✓
Sicherheitsprofile für Microsoft Intune-App erstellen und bearbeiten	✓	✓		
Sicherheitsprofile für Microsoft Intune-App löschen	✓	✓		
Layoutprofile für Startbildschirm anzeigen	✓	✓	✓	✓

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Layoutprofile für Startbildschirm erstellen und bearbeiten	✓	✓		
Layoutprofile für Startbildschirm löschen	✓	✓		
Enterprise Identity-Authentifizierungsrichtlinie anzeigen	✓	✓		
Enterprise Identity-Authentifizierungsrichtlin erstellen und bearbeiten	✓	✓		
Enterprise Identity-Authentifizierungsrichtlinie löschen	✓	✓		
Enterprise Identity-Authentifizierungsrichtlin Benutzern und Gruppen zuweisen	✓	✓		

Apps

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Apps und App-Gruppen anzeigen	✓	✓	✓	✓
Apps und App-Gruppen erstellen und bearbeiten	✓	✓		
Apps und App-Gruppen löschen	✓	✓		
App-Daten exportieren	✓	✓	✓	✓
Benutzern Apps und App-Gruppen zuweisen	✓	✓	✓	✓

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Benutzergruppen Apps und App-Gruppen zuweisen	✓	✓	✓	✓
Gerätegruppen Apps und App-Gruppen zuweisen	✓	✓	✓	✓
Apps und App-Gruppen freigegebenen Gerätegruppen zuweisen	✓	✓		
Apps und App-Gruppen öffentlichen Gerätegruppen zuweisen	✓	✓		
Einstellungen für App-Bewertungen und Rezensionen bearbeiten	✓	✓		
Löschen von App-Bewertungen und Rezensionen	✓	✓	✓	✓
Rangordnung der App-Installationen anzeigen	✓	✓	✓	✓
Rangordnung der App-Installationen bearbeiten	✓	✓		
App-Lizenzen anzeigen	✓	✓	✓	✓
App-Lizenzen erstellen	✓	✓		
App-Lizenzen bearbeiten	✓	✓		
App-Lizenzen löschen	✓	✓		
Apps oder App-Gruppen App-Lizenzen zuweisen	✓	✓	✓	✓

Gesperrte Apps

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Gesperrte Apps anzeigen	✓	✓	✓	✓
Gesperrte Apps erstellen	✓	✓		
Gesperrte Apps löschen	✓	✓		

Persönliche Apps

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Persönliche Apps anzeigen	✓	✓		

Einstellungen

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Allgemeine Einstellungen anzeigen	✓	✓	✓	✓
Standards der Aktivierung bearbeiten	✓	✓		
E-Mail-Vorlagen erstellen und bearbeiten	✓	✓		
E-Mail-Vorlagen löschen	✓	✓		
Konsoleneinstellungen bearbeiten	✓	✓		
Sprache für automatisierte E-Mails bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Einstellung der Selbstbedienungskonsole bearbeiten	✓	✓		
Sicherung des geschäftlichen Bereichs erstellen und Einstellungen wiederherstellen ¹	✓	✓		
Sicherung des geschäftlichen Bereichs löschen und Einstellungen wiederherstellen ¹	✓	✓		
Standardvariablen bearbeiten ¹	✓	✓		
Anmeldungshinweise bearbeiten ¹	✓	✓		
Benutzerdefinierte Variablen bearbeiten	✓	✓		
Organisationshinweise bearbeiten	✓	✓		
E-Mail-Domänen bearbeiten	✓	✓		
Einstellungen für Standortbestimmung bearbeiten	✓	✓		
Einstellungen für benutzerdefinierte Konsole bearbeiten	✓	✓		
Einstellungen zum Ablauf des Löschbefehls bearbeiten	✓	✓		
Nachweiseinstellungen bearbeiten	✓	✓		
Zertifikateinstellungen bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Ereignisbenachrichtigung erstellen und bearbeiten	✓	✓		
Ereignisbenachrichtigungen löschen	✓	✓		
Geräte-Supportmeldungen bearbeiten	✓	✓		
Zertifikatsbasierte Authentifizierungseinstellungen bearbeiten ¹	✓			
Zugriffseinstellungen für öffentliche Webservices bearbeiten	✓			
App-Verwaltung anzeigen	✓	✓	✓	✓
BlackBerry World for Work bearbeiten	✓	✓		
Speicher für interne Apps bearbeiten ¹	✓	✓		
Bearbeiten von Work Apps für iOS	✓	✓		
Windows 10-Apps bearbeiten	✓	✓		
Standardeinstellungen für App-Bewertungen und Rezensionen bearbeiten	✓	✓		
Externe Integrationseinstellungen anzeigen	✓	✓	✓	✓
Einstellungen für Apple-Push-Benachrichtigungen bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Einstellungen des SMTP-Servers bearbeiten ¹	✓	✓		
Apple DEP-Einstellungen bearbeiten	✓	✓		
BlackBerry 2FA-Servereinstellungen bearbeiten	✓	✓		
BlackBerry Connectivity Node-Einstellungen bearbeiten ²	✓	✓		
Token für Einmalkennwort anzeigen	✓	✓	✓	✓
Token für Einmalkennwort erstellen und bearbeiten	✓	✓		
Einstellungen für Unternehmensverzeichnis bearbeiten	✓	✓		
Microsoft Intune-Einstellungen bearbeiten	✓	✓		
Einstellungen zum Microsoft Exchange-Gatekeeping bearbeiten	✓	✓		
Einstellungen für geschäftliches Android-Profil bearbeiten	✓	✓		
Einstellungen für Zertifizierungsstelle bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Einstellungen für die Samsung Knox-Massenregistrierung bearbeiten	✓	✓		
Vertrauenswürdige Zertifikate anzeigen	✓	✓		
Vertrauenswürdige Zertifikate hinzufügen	✓	✓		
Vertrauenswürdige Zertifikate löschen	✓	✓		
BlackBerry Connectivity Node-Server anzeigen	✓	✓		
BlackBerry Connectivity Node-Server erstellen und bearbeiten	✓	✓		
BlackBerry Connectivity Node-Server löschen	✓	✓		
BlackBerry Secure Gateway-Einstellungen anzeigen	✓	✓		
BlackBerry Secure Gateway-Einstellungen bearbeiten	✓	✓		
Administratorbenutzer und -rollen anzeigen	✓	✓	✓	✓
Lizenzierungszusammen anzeigen	✓	✓	✓	✓
Lizenz Einstellungen bearbeiten	✓	✓		
Migrationseinstellungen anzeigen	✓	✓		
Migrationseinstellungen bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Infrastruktureinstellungen anzeigen	✓	✓	✓	
Protokollierungseinstellungen bearbeiten ¹	✓	✓		
Serverseitige Proxyeinstellungen bearbeiten ¹	✓	✓		
Server anzeigen ¹	✓	✓		
Server bearbeiten ¹	✓	✓		
Server löschen ¹	✓	✓		
Server verwalten ¹	✓	✓		
Überwachungseinstellungen anzeigen ¹	✓	✓		
Überwachungseinstellungen bearbeiten und Daten entfernen ¹	✓	✓		
BlackBerry Secure Connect Plus-Einstellungen anzeigen ¹	✓	✓		
BlackBerry Secure Connect Plus-Einstellungen bearbeiten ¹	✓	✓		
Serverzertifikate anzeigen ¹	✓	✓		
Serverzertifikate aktualisieren ¹	✓	✓		
BlackBerry Control-Einstellungen anzeigen	✓	✓	✓	✓
BlackBerry Control-Einstellungen bearbeiten	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
BlackBerry Dynamics NOC-Proxyservereinstellungen anzeigen ¹	✓	✓	✓	✓
BlackBerry Dynamics NOC-Proxyservereinstellungen bearbeiten ¹	✓	✓	✓	✓
SNMP-Einstellungen bearbeiten ¹	✓	✓		
IT-Richtlinienpaket und Geräte-Metadaten importieren ¹	✓			
Einstellungen für Collaboration Service anzeigen ¹	✓	✓	✓	✓
Einstellungen für Collaboration Service bearbeiten ¹	✓	✓		
BlackBerry Dynamics-Einstellungen anzeigen	✓	✓	✓	✓
BlackBerry Dynamics-App-Dienste anzeigen	✓	✓		
BlackBerry Dynamics-App-Dienste bearbeiten	✓			
BlackBerry Dynamics-App-Dienste erstellen	✓			
BlackBerry Dynamics-App-Dienste löschen	✓			
BlackBerry Dynamics-Servereigenschaften anzeigen ¹	✓	✓		
BlackBerry Dynamics-Servereigenschaften bearbeiten ¹	✓			

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
BlackBerry Dynamics Direct Connect-Einstellungen anzeigen	✓	✓		
BlackBerry Dynamics Direct Connect-Einstellungen bearbeiten	✓			
BlackBerry Dynamics-Serverclustereinstellungen anzeigen ¹	✓	✓		
BlackBerry Dynamics-Serverclustereinstellungen bearbeiten ¹	✓			
BlackBerry Dynamics-Berichte anzeigen	✓	✓	✓	
BlackBerry Dynamics-Kommunikationseinstellungen anzeigen ¹	✓	✓	✓	
BlackBerry Dynamics-Kommunikationseinstellungen bearbeiten ¹	✓			
BEMS-E-Mail-Einstellungen anzeigen ²	✓	✓		
BEMS-E-Mail-Einstellungen bearbeiten ²	✓			
BEMS Docs-Einstellungen anzeigen ²	✓	✓		
BEMS Docs-Einstellungen bearbeiten ²	✓			
Enterprise Identity-Einstellungen anzeigen	✓	✓		

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Enterprise Identity-Enterprise-Einstellungen anzeigen	✓	✓		
Enterprise Identity-Enterprise-Einstellungen bearbeiten	✓	✓		
Enterprise Identity-Serviceeinstellungen anzeigen	✓	✓		
Enterprise Identity-Serviceeinstellungen bearbeiten	✓	✓		

¹ nur lokale Umgebungen

² nur Cloud-Umgebungen

Dashboard

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Dashboard anzeigen	✓	✓	✓	✓

Überwachung

Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Systemüberwachungsprotokolle anzeigen ¹	✓	✓		
Protokolle zur Geräteleistung anzeigen ¹	✓	✓		

¹ nur lokale Umgebungen


Workspaces


Berechtigung	Sicherheitsadministrat	Enterprise-Administrator	Senior Helpdesk	Junior Helpdesk
Unternehmensadministrator	✓			
Helpdesk-Administrator	✓			
Audit-Helpdesk-Administrator	✓			

Erstellen einer benutzerdefinierten Administratorrolle

Wenn die vorkonfigurierten Administratorrollen nicht die Anforderungen Ihres Unternehmens erfüllen, können Sie benutzerdefinierte erstellen. Außerdem können Sie benutzerdefinierte Rollen erstellen, um administrative Aufgaben auf eine definierte Liste von Benutzergruppen zu beschränken. So können Sie beispielsweise eine Rolle für neue Administratoren erstellen, die deren Berechtigungen auf eine Benutzergruppe nur zu Schulungszwecken beschränkt.

Bevor Sie beginnen:

- Nur Sicherheitsadministratoren können eine benutzerdefinierte Rolle erstellen.
 - Lesen Sie [Berechtigungen für vorkonfigurierte Administratorrollen](#).
1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Einstellungen > Administratoren > Rollen**.
 2. Klicken Sie auf .
 3. Geben Sie einen Namen und eine Beschreibung für die Rolle ein.
 4. Um Berechtigungen einer anderen Rolle zu kopieren, klicken Sie auf eine Rolle in der Dropdown-Liste **Berechtigungen von Rolle übernommen**.
 5. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Administratoren mit dieser Rolle ermöglichen, alle Unternehmensverzeichnisse zu durchsuchen.	Wählen Sie die Option Alle Firmenverzeichnisse aus.
Administratoren mit dieser Rolle ermöglichen, ausgewählte Unternehmensverzeichnisse zu durchsuchen.	<ol style="list-style-type: none"> a. Wählen Sie die Option Nur ausgewählte Unternehmensverzeichnisse aus. b. Klicken Sie auf Verzeichnisse auswählen. c. Wählen Sie mindestens ein Verzeichnis aus, und klicken Sie auf . d. Klicken Sie auf Speichern.

6. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Administratoren mit dieser Rolle ermöglichen, alle Benutzer und Gruppen zu verwalten	Wählen Sie die Option Alle Gruppen und Benutzer aus.
Administratoren mit dieser Rolle ermöglichen, ausgewählte Gruppen zu verwalten	<ul style="list-style-type: none"> a. Wählen Sie die Option Nur ausgewählte Gruppen aus. b. Klicken Sie auf Gruppen auswählen. c. Wählen Sie mindestens eine Gruppe aus, und klicken Sie auf ➔. d. Klicken Sie auf Speichern.

7. Konfigurieren Sie die Berechtigungen für Administratoren mit dieser Rolle.

8. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Informationen zum Zuweisen von Rangordnungen zu Rollen, zum Ändern von Rolleneinstellungen oder zum Löschen einer Rolle finden Sie unter [Verwalten von Administratorrollen](#).


Verwalten von Administratorrollen

Nachdem Sie eine Administratorrolle erstellt haben, können Sie der Rolle eine Rangordnung zuweisen, die Berechtigungen der Rolle ändern oder die Rolle löschen. BlackBerry UEM verwendet Rangordnungen, um festzulegen, welche Rolle einem Administrator zugewiesen wird, wenn er Mitglied mehrerer Benutzergruppen ist, die verschiedene Rollen haben. Wenn eine Rolle einem Benutzerkonto direkt zugewiesen wird, hat sie Vorrang vor einer einer Benutzergruppe zugewiesenen Rolle. Wenn ein Administrator Mitglied mehrerer Benutzergruppen mit verschiedenen Rollen ist, weist UEM die Rolle mit der höchsten Rangordnung zu.

Bevor Sie beginnen: Nur Sicherheitsadministratoren können Administratorrollen verwalten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Administratoren > Rollen**.

2. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Einer Rolle eine Rangordnung zuweisen.	<ul style="list-style-type: none"> a. Verwenden Sie die Pfeile, um die Rangordnung der Rolle zu ändern. b. Klicken Sie auf Speichern.
Ändern der Rolleneinstellungen.	<ul style="list-style-type: none"> a. Klicken Sie auf den Namen der Rolle, die Sie ändern möchten. b. Klicken Sie auf Bearbeiten. c. Nehmen Sie die Änderungen vor. d. Klicken Sie auf Speichern.
Löschen einer Rolle.	<ul style="list-style-type: none"> a. Klicken Sie auf den Namen der Rolle, die Sie löschen möchten. b. Klicken Sie auf .



Erstellen eines Administrators

Sie können einen Administrator erstellen, indem Sie einem Benutzerkonto oder einer Benutzergruppe eine Administratorrolle zuweisen. Die Benutzergruppe kann eine per Verzeichnis verknüpfte Gruppe oder eine lokale Gruppe sein. Sie können eine Rolle einem Benutzer und jeder Gruppe hinzufügen, der er angehört, aber BlackBerry UEM weist nur eine Rolle dem Benutzer zu.

Wenn eine Rolle einem Benutzerkonto oder einer Benutzergruppe zugewiesen wird, sendet UEM den Administratoren eine E-Mail mit deren Benutzernamen und einem Link zur Verwaltungskonsolle. UEM sendet den Administratoren zudem eine separate E-Mail mit deren Kennwort für die Verwaltungskonsolle. Wenn ein Administrator noch kein Kontokennwort hat, generiert UEM ein temporäres Kennwort und sendet es an den Administrator.


Bevor Sie beginnen:

- Nur Sicherheitsadministratoren können Administratoren erstellen.
 - [Erstellen einer benutzerdefinierten Administratorrolle](#), falls erforderlich.
1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Einstellungen > Administratoren**.
 2. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Zuweisen einer Rolle zu einem Benutzerkonto.	<ol style="list-style-type: none">a. Klicken Sie auf Benutzer.b. Klicken Sie auf .c. Klicken Sie auf den Namen des Benutzerkontos, dem Sie die Rolle zuweisen möchten.
Zuweisen einer Rolle zu einer Benutzergruppe.	<ol style="list-style-type: none">a. Klicken Sie auf Gruppen.b. Klicken Sie auf .c. Klicken Sie auf den Namen der Benutzergruppe, der Sie die Rolle zuweisen möchten.

3. Klicken Sie in der Dropdown-Liste **Rolle** auf die Rolle, die Sie zuweisen möchten.
4. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Um eine zugewiesene Rolle zu ändern, klicken Sie auf den Namen eines Benutzerkontos oder einer Benutzergruppe, klicken Sie auf die Rolle, die Sie zuweisen möchten, und klicken Sie auf **Speichern**.
- Um einen Administrator zu löschen, wählen Sie das Benutzerkonto oder die Benutzergruppe aus, aus dem/der Sie die Rolle entfernen möchten, und klicken Sie auf  > **Löschen**.

Erstellen und Verwalten von Benutzerkonten

Sie können Benutzerkonten direkt in BlackBerry UEM oder, falls Sie UEM mit Ihrem Unternehmensverzeichnis verbunden haben, über Ihr Unternehmensverzeichnis erstellen. Sie können auch eine CSV-Datei verwenden, um UEM mehrere Benutzerkonten gleichzeitig hinzuzufügen.

Nachdem Sie Benutzerkonten erstellt haben, können Sie Dienste für Benutzer aktivieren, Benutzer zu Gruppen hinzufügen, Geräte von Benutzern auf UEM aktivieren und Mitteilungen an Benutzer senden.

Erstellen eines Benutzerkontos

Bevor Sie beginnen:

- Wenn Sie einen Verzeichnisbenutzer hinzufügen möchten, stellen Sie sicher, dass BlackBerry UEM mit Ihrem Unternehmensverzeichnis verbunden ist. Informationen über die Verknüpfung von UEM mit einem Unternehmensverzeichnis und die Aktivierung von per Verzeichnis verknüpften Gruppen finden Sie unter [Verbinden mit dem Verzeichnis Ihres Unternehmens](#) in der Dokumentation zur Konfiguration.
 - Wenn Sie möchten, dass Benutzer den [BlackBerry Workspaces-Dienst](#) nutzen können, stellen Sie sicher, dass das Workspaces-Plug-in für UEM auf jeder Instanz von UEM in Ihrer Umgebung installiert ist.
1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte > Benutzer hinzufügen**.
 2. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Hinzufügen eines Verzeichnisbenutzers	<ol style="list-style-type: none">a. Suchen Sie auf der Registerkarte Unternehmensverzeichnis nach dem Verzeichnisbenutzer, den Sie hinzufügen möchten. Sie können nach Vorname, Nachname, Anzeigenname, Benutzername oder E-Mail-Adresse suchen.b. Wählen Sie in den Suchergebnissen das Benutzerkonto aus.
Hinzufügen eines lokalen Benutzers	<ol style="list-style-type: none">a. Geben Sie auf der Registerkarte Lokal den Vor- und Nachnamen des Benutzers an.b. Optional können Sie den Anzeigenamen des Benutzers bearbeiten.c. Geben Sie im Feld Benutzername einen einmaligen Benutzernamen ein.d. Geben Sie im Feld E-Mail-Adresse eine Kontakt-E-Mail-Adresse für das Benutzerkonto ein. Die E-Mail-Adresse für das Benutzerkonto ist erforderlich, wenn Sie einen Dienst wie Workspaces oder die Geräteverwaltung aktivieren.e. Klicken Sie optional auf Weitere Benutzerdetails und füllen Sie die Felder nach Bedarf aus.
Hinzufügen eines BlackBerry Online Account-Benutzers (nur UEM Cloud)	<ol style="list-style-type: none">a. Geben Sie auf der Registerkarte Nicht-Verzeichnis den Vor- und Nachnamen des Benutzers an.b. Optional können Sie den Anzeigenamen des Benutzers bearbeiten.c. Geben Sie im Feld E-Mail-Adresse eine Kontakt-E-Mail-Adresse für das Benutzerkonto ein. Die E-Mail-Adresse für das Benutzerkonto ist erforderlich, wenn Sie einen Dienst wie Workspaces oder die Geräteverwaltung aktivieren.d. Klicken Sie optional auf Weitere Benutzerdetails und füllen Sie die Felder nach Bedarf aus.

3. Wenn in UEM lokale Gruppen vorhanden sind und Sie ein Benutzerkonto zu Gruppen hinzufügen möchten, klicken Sie auf eine oder mehrere Gruppen in der Liste **Verfügbare Gruppen** und dann auf ➔.
Wenn Sie ein Benutzerkonto erstellen, können Sie es nur lokalen Gruppen hinzufügen. Wenn das Benutzerkonto ein Mitglied einer per Verzeichnis verknüpften Gruppe ist, wird es automatisch dieser Gruppe zugewiesen, wenn die Synchronisierung zwischen UEM und Ihrem Unternehmensverzeichnis erfolgt.
4. Wählen Sie in einer Cloud-Umgebung unter **UEM Self-Service** entweder **BlackBerry Online Account** oder **Lokales UEM-Benutzerkonto** aus. Wenn Sie ein lokales UEM-Benutzerkonto auswählen, erstellen Sie ein Kennwort für BlackBerry UEM Self-Service. Wenn der Benutzer einer Administratorrolle zugeordnet ist, können Sie auch das Kennwort für den Zugriff auf die Verwaltungskonsole verwenden.
5. Wenn Sie einen lokalen Benutzer in einer lokalen Umgebung hinzufügen, erstellen Sie im Feld **Kennwort** ein Kennwort für UEM Self-Service. Wenn der Benutzer einer Administratorrolle zugeordnet ist, können Sie auch das Kennwort für den Zugriff auf die Verwaltungskonsole verwenden.
6. Aktivieren Sie im Abschnitt **Aktivierte Services** das Kontrollkästchen **Benutzer für die Geräteverwaltung aktivieren**.
7. Wenn das Workspaces-Plug-in für UEM in der Domäne installiert ist, tun Sie zum Aktivieren des Workspaces-Dienstes Folgendes:
 - a) Aktivieren Sie im Abschnitt **BlackBerry Workspaces** das Kontrollkästchen **BlackBerry Workspaces aktivieren**. Standardmäßig erhalten Benutzer, die für den Workspaces-Dienst aktiviert sind, die Besucherrolle.
 - b) Wählen Sie mindestens eine Benutzerrolle aus, und klicken Sie auf ➔.
8. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Lassen Sie Benutzer Geräte mit dem Aktivierungsprofil aktivieren, das ihnen derzeit zugewiesen ist.	<ol style="list-style-type: none"> a. Wählen Sie in der Dropdown-Liste Aktivierungsoption Standardmäßige Geräteaktivierung aus. b. Wählen Sie in der Dropdown-Liste Aktivierungskennwort aus, ob Sie das Kennwort selbst auswählen oder es automatisch erzeugen lassen möchten. c. Sie haben optional die Möglichkeit, den Ablauf des Aktivierungszeitraums zu ändern. d. Wenn Sie möchten, dass das Aktivierungskennwort nur für eine Geräteaktivierung gültig ist, wählen Sie Aktivierungszeitraum endet nach der Aktivierung des ersten Geräts aus. e. Wählen Sie in der Dropdown-Liste Vorlage für Aktivierungs-E-Mails die Vorlage aus, die Sie für die Aktivierungs-E-Mail verwenden möchten.
Koppeln Sie ein Aktivierungskennwort mit einem bestimmten Aktivierungsprofil.	<ol style="list-style-type: none"> a. Klicken Sie in der Dropdown-Liste Aktivierungsoption auf Geräteaktivierung mit einem bestimmten Aktivierungsprofil. b. Wählen Sie in der Dropdown-Liste Aktivierungsprofil das Aktivierungsprofil aus, das Sie mit einem Kennwort koppeln möchten. c. Wählen Sie in der Dropdown-Liste Aktivierungskennwort aus, ob Sie das Kennwort selbst auswählen oder es automatisch erzeugen lassen möchten. d. Sie haben optional die Möglichkeit, den Ablauf des Aktivierungszeitraums zu ändern. e. Wenn Sie möchten, dass das Aktivierungskennwort nur für eine Geräteaktivierung gültig ist, wählen Sie Aktivierungszeitraum endet nach der Aktivierung des ersten Geräts aus. f. Wählen Sie in der Dropdown-Liste Vorlage für Aktivierungs-E-Mails die Vorlage aus, die Sie für die Aktivierungs-E-Mail verwenden möchten.

Aufgabe	Schritte
Benutzern erlauben, nur BlackBerry Dynamics-Apps zu aktivieren.	<ol style="list-style-type: none"> Wählen Sie in der Dropdown-Liste Activation option BlackBerry Dynamics access key generation aus. Wählen Sie in der Dropdown-Liste Anzahl der zu generierenden Zugriffsschlüssel die Anzahl der Schlüssel aus. Jeder Schlüssel kann nur einmal zur Aktivierung einer BlackBerry Dynamics-App genutzt werden. Wählen Sie die Anzahl der Tage aus, an denen der Zugriffsschlüssel gültig sein soll. Wählen Sie in der Dropdown-Liste Vorlage für Aktivierungs-E-Mails die Vorlage aus, die Sie für die Aktivierungs-E-Mail verwenden möchten.
Den Benutzer nur zu UEM hinzufügen.	Wählen Sie in der Dropdown-Liste Aktivierungsoption Nicht festlegen aus.

9. Wenn Sie benutzerdefinierte Variablen verwenden, erweitern Sie den Punkt **Benutzerdefinierte Variablen**, und geben Sie die entsprechenden Werte für die definierten Variablen ein.

10. Führen Sie einen der folgenden Schritte aus:

- Um Das Benutzerkonto zu speichern, klicken Sie auf **Speichern**.
- Um das Benutzerkonto zu speichern und ein weiteres zu erstellen, klicken Sie auf **Speichern und neu**.

Erstellen von Benutzerkonten aus einer .csv-Datei

Sie können Benutzerkonten aus einer .csv-Datei in BlackBerry UEM importieren, um mehrere Benutzerkonten auf einmal zu erstellen. Sie können die .csv-Datei manuell erstellen, indem Sie eine .csv-Beispieldatei verwenden, die Sie von der Verwaltungskonsole herunterladen können (**Benutzer > Alle Benutzer > Benutzer hinzufügen > Importieren > .csv-Beispieldatei herunterladen**).

Je nach Anforderungen können Sie in der .csv-Datei Gruppenmitgliedschaften und Aktivierungseinstellungen für die Benutzerkonten angeben, indem Sie die folgenden Spalten in der .csv-Datei aufnehmen:

Spaltenüberschrift	Beschreibung
Gruppenmitgliedschaft	<p>Weisen Sie jedem Benutzerkonto eine oder mehrere Benutzergruppen zu.</p> <p>Trennen Sie mehrere Benutzergruppen mit einem Semikolon (;).</p> <p>Wenn Sie beim Importieren der Datei die Spalte „Gruppenmitgliedschaft“ nicht aufnehmen, haben Sie die Möglichkeit, die Gruppe auszuwählen, der alle importierten Benutzerkonten hinzugefügt werden sollen.</p>
MDM (BlackBerry UEM)	Geben Sie an, ob der Benutzer für MDM aktiviert ist. Um einen Benutzer für MDM zu aktivieren, geben Sie „Aktiviert“ ein.
Aktivierungskennwort	<p>Das Aktivierungskennwort festlegen.</p> <p>Dieser Wert ist erforderlich, wenn der Wert für die „Generierung des Aktivierungskennworts“ auf „Manuell“ festgelegt ist.</p>
Aktivierungsvorlage	Legen Sie den Namen der Vorlage der Aktivierungs-E-Mail fest, die Sie dem Benutzer senden möchten. Wenn Sie keinen Namen angeben, wird die Standard-E-Mail-Aktivierungsvorlage verwendet.

Spaltenüberschrift	Beschreibung
Ablauf des Aktivierungskennworts	Geben Sie die Zeit in Sekunden an, die das Aktivierungskennwort gültig ist, bevor es abläuft.
Generierung des Aktivierungskennworts	<p>Wählen Sie eine der folgenden Optionen:</p> <ul style="list-style-type: none"> • Automatisch: Das Aktivierungskennwort wird automatisch erstellt und an den Benutzer gesendet. (Standard) • Manuell: Das Aktivierungskennwort wird in der Spalte „Aktivierungskennwort“ eingerichtet. • Ignorieren: Es wird kein Aktivierungskennwort generiert.
Aktivierungs-E-Mail senden	<p>Wählen Sie eine der folgenden Optionen:</p> <ul style="list-style-type: none"> • Wahr: Die Aktivierungs-E-Mail wird an den Benutzer gesendet. • Falsch: Die Aktivierungs-E-Mail wird nicht an den Benutzer gesendet. <p>Wenn „Generierung des Aktivierungskennworts“ auf „Automatisch“ gesetzt ist, wird die Aktivierungs-E-Mail unabhängig vom Wert in dieser Spalte an den Benutzer gesendet. Wenn der Wert „Generierung des Aktivierungskennworts“ auf „Manuell“ gesetzt ist und der Wert leer ist, gilt der Standardwert „Richtig“. Wenn der Wert für „Aktivierungskennwort generieren“ „Ignorieren“ lautet, erhält der Benutzer keine Self-Service-Aktivierungs-E-Mail.</p>
Benutzertyp	<p>Diese Spalte ist immer dann erforderlich, wenn die .csv-Datei sowohl lokale Benutzerkonten als auch Verzeichnisbenutzerkonten enthält. Wählen Sie eine der folgenden Optionen:</p> <ul style="list-style-type: none"> • L: Lokale Benutzerkonten • D: Verzeichnisbenutzerkonten
Verzeichnis-UID	<p>Diese Spalte ist eine Alternative zum Eingeben der E-Mail-Adresse für Verzeichnisbenutzerkonten. Standardmäßig wird die E-Mail-Adresse zum Überprüfen der Verzeichnisbenutzerkonten verwendet. Sie können aber angeben, dass stattdessen die Verzeichnis-UID verwendet wird. Wenn das Benutzerkonto nicht anhand der Verzeichnis-UID überprüft werden kann, wird ein Fehler gemeldet.</p> <p>Wenn Sie einen Verzeichnis-UID-Wert für einen Ihrer Benutzer hinzufügen, muss die Spaltenüberschrift die Verzeichnis-UID enthalten, und alle Reihen der .csv-Datei müssen entweder eine Verzeichnis-UID oder einen leeren Platzhalter (.) für die Verzeichnis-UID-Spalte enthalten.</p>

Hinzufügen von Benutzerkonten zu UEM mithilfe einer .csv-Datei

Bevor Sie beginnen:

- Bereiten Sie die .csv-Datei vor. Weitere Informationen finden Sie unter [Erstellen von Benutzerkonten aus einer .csv-Datei](#).
 - Wenn die .csv-Datei Verzeichnisbenutzerkonten enthält, überprüfen Sie, ob BlackBerry UEM mit Ihrem Unternehmensverzeichnis verbunden ist.
1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Benutzer**.
 2. Klicken Sie auf der Registerkarte **Alle Benutzer** oder **Verwaltete Geräte** auf **Benutzer hinzufügen**.
 3. Klicken Sie auf der Registerkarte **Importieren** auf **Durchsuchen**, und navigieren Sie zur .csv-Datei.

4. Klicken Sie auf **Laden**.
5. Wenn die .csv-Datei nicht die Spalte „Gruppenmitgliedschaft“ verwendet und Sie Benutzerkonten zu Gruppen hinzufügen möchten, wählen Sie eine oder mehrere Gruppen in der Liste **Verfügbare Gruppen** aus, und klicken Sie auf ➔. Klicken Sie auf **Weiter**.



Wenn Sie die .csv-Datei importieren, werden alle Benutzerkonten den von Ihnen ausgewählten lokalen Gruppen hinzugefügt. Wenn ein Benutzerkonto ein Mitglied einer per Verzeichnis verknüpften Gruppe ist, wird es automatisch dieser Gruppe zugewiesen, wenn die Synchronisierung zwischen UEM und Ihrem Unternehmensverzeichnis erfolgt.

6. Überprüfen Sie die Liste der Benutzerkonten, und tun Sie eines der folgenden Dinge:
 - Um die Fehler für Konten ungültiger Verzeichnisbenutzer zu korrigieren, klicken Sie auf **Abbrechen**, nehmen Sie Korrekturen an der Datei vor, und laden Sie sie erneut hoch.
 - Zum Hinzufügen der gültigen Benutzerkonten klicken Sie auf **Import**. Ungültige Verzeichnisbenutzerkonten werden ignoriert.

Aktivieren von Diensten für einen Benutzer

Wenn BlackBerry UEM für mindestens einen Dienst (z. B. Workspaces, BBM Enterprise oder Enterprise Identity) aktiviert ist, können Sie einen Dienst für einen Benutzer aktivieren.


1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Alle Benutzer**.
2. Suchen Sie nach einem Benutzerkonto, und klicken Sie darauf.
3. Auf der Seite mit den Detailinformationen werden die verfügbaren Dienste unter dem Namen des Benutzers aufgeführt.
4. Wenn ein Dienst derzeit nicht aktiviert ist, wird er mit einem +-Symbol aufgeführt. Klicken Sie auf +, um den Dienst hinzuzufügen.
5. Konfigurieren Sie den Dienst nach Bedarf, und speichern Sie.

Wenn Sie fertig sind: Wenn Sie einen Dienst von einem Benutzer entfernen möchten, klicken Sie auf . Klicken Sie beim Dienst, den Sie ändern möchten, auf . Bevor Sie MDM-Steuerelemente entfernen können, müssen Sie die für den Benutzer aktivierten Geräte entfernen. Bevor Sie den Enterprise Identity-Dienst löschen können, müssen Sie alle Enterprise Identity-Zuweisungen vom Benutzer entfernen.



Hinzufügen von Benutzern zu Benutzergruppen

Weitere Informationen zu Benutzergruppen finden Sie unter [Erstellen und Verwalten von Benutzergruppen](#). Beachten Sie, dass Sie die Mitgliedschaft eines Benutzers in einer per Verzeichnis verknüpften Gruppe nicht ändern können.

Bevor Sie beginnen: Zum Hinzufügen eines Benutzers, dem eine Administratorrolle zugewiesen ist, zu einer Benutzergruppe müssen Sie Sicherheitsadministrator sein.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die Sie den Benutzergruppen hinzufügen möchten.
3. Klicken Sie auf .
4. Wählen Sie in der Liste **Verfügbare Gruppen** eine oder mehrere Gruppen aus, und klicken Sie auf ➔.
5. Klicken Sie auf **Speichern**.







Wenn Sie fertig sind:

- Um zu ändern, zu welcher Benutzergruppe ein Benutzer gehört, klicken Sie auf den Namen des Benutzerkontos, dessen Mitgliedschaft Sie ändern möchten. Klicken Sie auf , und verwenden Sie im Abschnitt **Gruppenmitgliedschaft** die Pfeile nach links und rechts, um den Benutzer zu Gruppen hinzuzufügen oder den Benutzer aus Gruppen zu entfernen.
- Um mehrere Benutzer aus einer Benutzergruppe zu entfernen, klicken Sie in der Menüleiste auf **Gruppen**. Klicken Sie auf die Benutzergruppe, aus welcher Sie die Benutzer entfernen möchten. Wählen Sie die Benutzer aus, die Sie entfernen möchten, und klicken Sie auf .

Verwalten von Benutzerkonten

Bevor Sie beginnen: [Erstellen eines Benutzerkontos](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Führen Sie einen der folgenden Schritte aus:
 - Um einen einzelnen Benutzer zu verwalten, suchen Sie nach einem Benutzerkonto, und klicken Sie darauf. Fahren Sie dann mit dem nächsten Schritt fort.
 - Um eine Aktion für mehrere Benutzerkonten gleichzeitig auszuführen, aktivieren Sie das Kontrollkästchen neben jedem Benutzerkonto, das Sie verwalten möchten. Klicken Sie auf eine Aktion oberhalb der Benutzerliste (Sie können beispielsweise die ausgewählten Benutzerkonten zu Benutzergruppen hinzufügen), und befolgen Sie die Anweisungen auf dem Bildschirm.
3. Führen Sie eine der folgenden Aktionen aus:



Aufgabe	Schritte
Bearbeiten der Informationen eines Benutzers.	<ol style="list-style-type: none"> Klicken Sie auf . Ändern des Benutzerkontos. Klicken Sie auf Speichern.
Hinzufügen eines Hinweises zu einem Benutzerkonto.	<ol style="list-style-type: none"> Klicken Sie auf . Geben Sie Hinweise ein. Die Hinweise, die Sie eingeben, werden automatisch im Benutzerkonto und nicht in einem einzelnen Gerät gespeichert.
Dem Benutzer eine IT-Richtlinie, ein Profil, eine App oder eine App-Gruppe zuweisen	<ol style="list-style-type: none"> Klicken Sie im entsprechenden Abschnitt auf . Wählen Sie IT-Richtlinie, Profil, App oder App-Gruppe aus, die Sie zuweisen möchten. Befolgen Sie die Anweisungen, und wählen Sie die entsprechenden Einstellungen aus, um die Zuweisung abzuschließen. Um eine IT-Richtlinie, ein Profil, eine App oder eine App-Gruppe von dem Benutzer zu entfernen, klicken Sie neben der Eigenschaft, die Sie löschen möchten, auf .
Synchronisieren der Informationen für einen Verzeichnisbenutzer	Klicken Sie auf  .
Löschen eines Benutzerkontos.	<ol style="list-style-type: none"> Klicken Sie auf . Klicken Sie auf Löschen.

Kommunikation an Benutzer senden

Sie können eine E-Mail, einschließlich einer E-Mail-Nachricht mit einem BlackBerry UEM Self-Service-Kennwort, an einen oder mehrere Benutzer senden. Wenn Sie ein Kennwort senden, werden die Kennwörter zufällig erstellt, und eine E-Mail-Nachricht, die das Kennwort enthält, wird an jeden Benutzer gesendet. In lokalen UEM-Umgebungen können Sie die E-Mail-Adresse des Absenders in den SMTP-Servereinstellungen konfigurieren.

Bevor Sie beginnen: Die Benutzer, an die Sie die E-Mail-Nachricht senden, müssen eine mit ihrem Benutzerkonto verknüpfte E-Mail-Adresse haben.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Aktivieren Sie das Kontrollkästchen neben jedem Benutzer, der die Nachricht erhalten soll.
3. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Senden einer E-Mail an Benutzer.	<ol style="list-style-type: none">a. Klicken Sie auf .b. Um eine Kopie der E-Mail an sich selbst oder an andere zu senden, klicken Sie auf CC, und geben Sie eine oder mehrere E-Mail-Adressen ein. Trennen Sie die Adressen durch Kommas oder Semikola.
Ein BlackBerry UEM Self-Service-Kennwort an Benutzer senden.	<ol style="list-style-type: none">a. Klicken Sie auf .b. Klicken Sie auf Fortfahren.

Erstellen und Verwalten von Benutzergruppen

Eine Benutzergruppe ist eine Zusammenfassung ähnlicher Benutzer, die gemeinsame Eigenschaften haben. Die Administration von Benutzern als Gruppe ist effizienter als die Administration von individuellen Benutzern, da die Eigenschaften für alle Mitglieder der Gruppe gleichzeitig hinzugefügt, geändert oder entfernt werden können. Benutzer können gleichzeitig zu mehr als einer Gruppe gehören. Wenn Sie eine Benutzergruppe erstellen und verwalten, können Sie IT-Richtlinien, Profile und Apps in der Verwaltungskonsole zuweisen. Sie können auch eine Gruppe als Mitglied einer anderen Gruppe definieren.

Sie können zwei Arten von Benutzergruppen erstellen:

- Per Verzeichnis verknüpfte Gruppen: Das sind mit Gruppen in Ihrem Unternehmensverzeichnis verknüpfte Gruppen. Nur Verzeichnisbenutzerkonten können Mitglieder in einer per Verzeichnis verknüpften Gruppe sein.
- Lokale Gruppen: Diese Gruppen werden in BlackBerry UEM erstellt und verwaltet, und Sie können ihnen sowohl lokale Benutzerkonten als auch Verzeichnisbenutzerkonten zuweisen.

UEM synchronisiert bei per Verzeichnis verknüpften Gruppen regelmäßig die Mitgliedschaft der Gruppe mit den verknüpften Unternehmensverzeichnisgruppen. Benutzer, die zum Unternehmensverzeichnis hinzugefügt oder daraus entfernt wurden, werden zur per Verzeichnis verknüpften Gruppe hinzugefügt bzw. daraus entfernt. Wenn Benutzer einer Unternehmensverzeichnisgruppe hinzugefügt werden, die mit einer per Verzeichnis verknüpften Gruppe verknüpft ist, werden ihnen die Eigenschaften zugewiesen, die der Gruppe zugewiesen sind. Wenn Benutzer aus der per Verzeichnis verknüpften Gruppe entfernt werden, werden die Eigenschaften vom Benutzer entfernt.



Jede per Verzeichnis verknüpfte Gruppe kann mit einem einzelnen Unternehmensverzeichnis verknüpft werden. Wenn UEM beispielsweise zwei Microsoft Active Directory-Verbindungen (A und B) hat und Sie eine per Verzeichnis verknüpfte Gruppe erstellen, die mit einer Verbindung A verknüpft ist, können Sie nur Verzeichnisgruppen der Verbindung A mit dieser Gruppe verknüpfen. Sie müssen neue per Verzeichnis verknüpfte Gruppen für andere Verzeichnisverbindungen erstellen.


Durch die Synchronisierung von per Verzeichnis verknüpften Gruppen werden keine Benutzer in UEM hinzugefügt oder gelöscht. Um zuzulassen, dass UEM Benutzerkonten erstellt, wenn neue Unternehmensverzeichnisbenutzer erstellt werden, müssen Sie [Onboarding aktivieren](#).

Erstellen einer per Verzeichnis verknüpften Gruppe

Sie können Benutzergruppen erstellen, die mit Gruppen in Ihrem Unternehmensverzeichnis verknüpft sind. BlackBerry UEM synchronisiert regelmäßig die Mitgliedschaft einer per Verzeichnis verknüpften Gruppe mit ihren verknüpften Unternehmensverzeichnisgruppen. Wenn Benutzer zur Unternehmensverzeichnisgruppe hinzugefügt oder daraus entfernt werden, werden sie zur per Verzeichnis verknüpften Gruppe hinzugefügt bzw. daraus entfernt. Die Profile, Richtlinien und Apps, die Sie der per Verzeichnis verknüpften Gruppe zuweisen, werden den Benutzern in dieser Gruppe zugewiesen. Wenn Benutzer aus der Gruppe entfernt werden, werden diese Eigenschaften entfernt.

Bevor Sie beginnen: [Aktivieren Sie per Verzeichnis verknüpfte Gruppen](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Gruppen > Benutzer**.
2. Klicken Sie auf .
3. Geben Sie den Gruppennamen ein.
4. Tun Sie im Feld **Verknüpfte Verzeichnisgruppen** Folgendes:
 - a) Klicken Sie auf .
 - b) Geben Sie den Namen oder partiellen Namen der Unternehmensverzeichnisgruppe ein, zu der Sie eine Verknüpfung erstellen möchten.


- c) Wenn mehr als eine Unternehmensverzeichnisverbindung vorhanden ist, wählen Sie Verbindung aus, die Sie suchen möchten. Nach dieser Auswahl wird die per Verzeichnis verknüpfte Gruppe permanent nur mit der ausgewählten Verbindung verknüpft.
 - d) Klicken Sie auf .
 - e) Wählen Sie die Unternehmensverzeichnisgruppe aus.
 - f) Klicken Sie auf **Hinzufügen**.
 - g) Aktivieren Sie bei Bedarf das Kontrollkästchen **Verschachtelte Gruppen verknüpfen**, damit die Verzeichniseinstellungen die Anzahl verschachtelter Gruppen steuern können. Um eine Verknüpfung mit allen verschachtelten Gruppen herzustellen, lassen Sie das Kontrollkästchen deaktiviert.
 - h) Wiederholen Sie diese Schritte, um zusätzliche Gruppen zu verknüpfen.
5. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Weisen Sie der per Verzeichnis verknüpften Gruppe eine Benutzerrolle zu.	<ul style="list-style-type: none"> a. Klicken Sie im Abschnitt Benutzerrolle auf +. b. Klicken Sie in der Dropdown-Liste auf den Namen der Benutzerrolle, die Sie der Gruppe zuweisen möchten. c. Klicken Sie auf Hinzufügen.
Zuweisen einer IT-Richtlinie oder eines Profils zu der per Verzeichnis verknüpften Gruppe.	<ul style="list-style-type: none"> a. Klicken Sie im Abschnitt IT-Richtlinie und -Profil auf +. b. Klicken Sie auf IT-Richtlinie oder auf einen Profiltyp. c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie oder des Profils, die bzw. das Sie der Gruppe zuweisen möchten. d. Klicken Sie auf Zuweisen.
Zuweisen einer App zu der per Verzeichnis verknüpften Gruppe.	<ul style="list-style-type: none"> a. Klicken Sie im Abschnitt Zugewiesene Apps auf +. b. Suchen Sie nach der App, die Sie zuweisen möchten, und wählen Sie sie aus. c. Klicken Sie auf Weiter. d. Führen Sie in der Dropdown-Liste Verfügbarkeit eine der folgenden Aktionen aus: <ul style="list-style-type: none"> • Um die App automatisch auf Geräten zu installieren und zu verhindern, dass Benutzer die App deinstallieren, klicken Sie auf Erforderlich. • Damit Benutzer die App installieren müssen und Apple VPP-Apps nicht automatisch aktualisieren können, wählen Sie Erforderlich ohne Updates aus. • Um Benutzern das Installieren und Deinstallieren der App zu gestatten, wählen Sie Optional. • Um Benutzern das Installieren und Entfernen der App zu gestatten und zu verhindern, dass Apple VPP-Apps sich automatisch aktualisieren, wählen Sie Optional ohne Updates aus. e. Wenn Sie auf iOS-Geräten „Per App VPN“-Einstellungen einer App oder einer App-Gruppe zuweisen möchten, wählen Sie in der Dropdown-Liste Per App VPN die Einstellungen aus, die mit der App oder der App-Gruppe verknüpft werden sollen. f. Klicken Sie auf Zuweisen.

6. Klicken Sie auf **Hinzufügen**.


Hinzufügen einer Unternehmensverzeichnisgruppe zu einer vorhandenen per Verzeichnis verknüpften Gruppe

Bevor Sie beginnen: Erstellen einer per Verzeichnis verknüpften Gruppe.

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Gruppen > Benutzer**.
2. Klicken Sie auf die per Verzeichnis verknüpfte Gruppe.
3. Klicken Sie auf der Registerkarte **Einstellungen** auf .
4. Klicken Sie im Abschnitt **Verknüpfte Verzeichnisgruppen** auf **+**.
5. Suchen Sie die Unternehmensverzeichnisgruppe, die Sie einer vorhandenen per Verzeichnis verknüpften Gruppe hinzufügen möchten, und wählen Sie sie aus.
6. Klicken Sie auf **Hinzufügen**.
7. Falls erforderlich, wählen Sie **Verschachtelte Gruppen verknüpfen** aus.

Erstellen einer lokalen Gruppe

Sie können eine lokale Benutzergruppe in BlackBerry UEM erstellen, der Sie IT-Richtlinien, Profile und Apps zuweisen können. Wenn Sie Benutzerkonten zur Gruppe hinzufügen, werden die Eigenschaften, die Sie der Gruppe zuweisen, jedem Mitglied der Gruppe zugewiesen. Sie können sowohl lokale Benutzerkonten als auch Verzeichnisbenutzerkonten einer lokalen Gruppe zuweisen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Gruppen > Benutzer**.
2. Klicken Sie auf .
3. Geben Sie einen Namen und eine Beschreibung für die Gruppe ein.
4. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Zuweisen einer Benutzerrolle zu der lokalen Gruppe.	<ol style="list-style-type: none">a. Klicken Sie im Abschnitt Benutzerrolle auf +.b. Klicken Sie in der Dropdown-Liste auf den Namen der Benutzerrolle, die Sie der Gruppe zuweisen möchten.c. Klicken Sie auf Hinzufügen.
Zuweisen einer IT-Richtlinie oder eines Profils zu der lokalen Gruppe.	<ol style="list-style-type: none">a. Klicken Sie im Abschnitt IT-Richtlinie und -Profile auf +.b. Klicken Sie auf IT-Richtlinie oder auf einen Profiltyp.c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie oder des Profils, die bzw. das Sie der Gruppe zuweisen möchten.d. Klicken Sie auf Zuweisen.

Aufgabe	Schritte
Zuweisen einer App zu der lokalen Gruppe.	<p>a. Klicken Sie im Abschnitt Zugewiesene Apps auf +.</p> <p>b. Suchen Sie nach der App, die Sie einer Gruppe zuweisen möchten, und wählen Sie diese aus.</p> <p>c. Klicken Sie auf Weiter.</p> <p>d. Führen Sie in der Dropdown-Liste Verfügbarkeit eine der folgenden Aktionen aus:</p> <ul style="list-style-type: none"> • Um die App automatisch auf Geräten zu installieren und zu verhindern, dass Benutzer die App deinstallieren, klicken Sie auf Erforderlich. Diese Option ist für BlackBerry-Apps nicht verfügbar. • Damit Benutzer die App installieren müssen und Apple VPP-Apps nicht automatisch aktualisieren können, wählen Sie Erforderlich ohne Updates aus. • Um Benutzern das Installieren und Deinstallieren der App zu gestatten, wählen Sie Optional. • Um Benutzern das Installieren und Entfernen der App zu gestatten und zu verhindern, dass Apple VPP-Apps sich automatisch aktualisieren, wählen Sie Optional ohne Updates aus. <p>Wenn eine App sowohl einem Benutzerkonto als auch der Benutzergruppe dieses Benutzerkontos zugewiesen ist, wird die Verfügbarkeit der App, die dem Benutzerkonto zugewiesen ist, vorrangig behandelt.</p> <p>e. Wenn Sie auf iOS-Geräten „Per App VPN“-Einstellungen einer App oder App-Gruppe zuweisen möchten, wählen Sie in der Dropdown-Liste Per App VPN die Einstellungen aus, die mit der App oder der App-Gruppe verknüpft werden sollen.</p> <p>f. Falls verfügbar, wählen Sie für iOS- und Android-Geräte eine App-Konfiguration aus, die der App zugewiesen werden soll.</p> <p>g. Wenn Sie Android Enterprise verwenden und Tracks für Apps in der Google Play-Konsole erstellt haben, wählen Sie einen Track, der der App zugewiesen werden soll.</p> <p>h. Klicken Sie auf Zuweisen.</p>

5. Klicken Sie auf **Hinzufügen**.

Hinzufügen von verschachtelten Gruppen zu einer Benutzergruppe

Wenn Sie eine Gruppe innerhalb einer Benutzergruppe verschachteln, übernehmen die Mitglieder der verschachtelten Gruppe die Eigenschaften der Benutzergruppe. Sie erstellen und verwalten die Verschachtelungsstruktur in BlackBerry UEM, und Sie können sowohl die per Verzeichnis verknüpften Gruppen als auch die lokalen Gruppen mit jeder Art von Benutzergruppe verschachteln. Wenn Sie einer Benutzergruppe eine verschachtelte Gruppe hinzufügen, werden alle Gruppen, die dieser verschachtelten Gruppe angehören, ebenfalls hinzugefügt.

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Gruppen > Benutzer**.
2. Suchen Sie nach dem Namen einer Benutzergruppe, und klicken Sie darauf.



3. Klicken Sie auf der Registerkarte **Verschachtelte Gruppen** auf **+**.
4. Wählen Sie eine oder mehrere Gruppen aus.
5. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Um verschachtelte Gruppen zu entfernen, die einer Benutzergruppe direkt zugewiesen sind, klicken Sie unter **Gruppen** auf den Namen der Benutzergruppe, aus der Sie eine Gruppe entfernen möchten. Klicken Sie auf der Registerkarte **Verschachtelte Gruppen** neben der verschachtelten Gruppe, die Sie entfernen möchten, auf **X**.

Verwalten einer Benutzergruppe

Bevor Sie beginnen: [Erstellen einer lokalen Gruppe](#) oder [Erstellen einer per Verzeichnis verknüpften Gruppe](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Gruppen > Benutzer**.
2. Suchen Sie die Benutzergruppe, die Sie verwalten möchten, und klicken Sie darauf.
3. Führen Sie eine der folgenden Aktionen aus:


Aufgabe	Schritte
Anzeigen von Informationen über eine Benutzergruppe.	<ol style="list-style-type: none"> a. Um die Benutzerkonten anzuzeigen, die der Gruppe zugewiesen sind, klicken Sie auf Benutzer. b. Um die verschachtelten Gruppen anzuzeigen, die der Gruppe zugewiesen sind, klicken Sie auf Verschachtelte Gruppen. c. Um die verknüpften Verzeichnisgruppen (falls verfügbar) oder die zugewiesenen Eigenschaften der Gruppe anzuzeigen, klicken Sie auf Einstellungen.
Ändern Sie den Namen oder die Beschreibung einer Benutzergruppe.	<ol style="list-style-type: none"> a. Klicken Sie auf . b. Ändern Sie den Namen oder die Beschreibung der Benutzergruppe. c. Klicken Sie auf Speichern.
Verwalten Sie die zugewiesenen Rollen, zugewiesenen Profile oder zugewiesenen Apps der Benutzergruppe.	<ol style="list-style-type: none"> a. Klicken Sie auf die Registerkarte Einstellungen. b. Um der Benutzergruppe eine Rolle, ein Profil oder eine App zuzuweisen, klicken Sie neben dem entsprechenden Abschnitt auf +. c. Um eine Rolle, ein Profil oder eine App aus der Benutzergruppe zu entfernen, klicken Sie neben der Eigenschaft, die Sie entfernen möchten, auf X.
Löschen einer Benutzergruppe	<ol style="list-style-type: none"> a. Klicken Sie auf . b. Klicken Sie auf Löschen.


Erstellen und Verwalten von Gerätegruppen

Eine Gerätegruppe ist eine Gruppe von Geräten mit gemeinsamen Attributen, wie zum Beispiel Modell und Hersteller, Betriebssystem und Version, Dienstanbieter und Eigentümer. BlackBerry UEM verschiebt auf Grundlage der von Ihnen definierten Attribute automatisch Geräte in die oder aus der Gerätegruppe.

Sie können die Gerätegruppen dazu nutzen, um bestimmten Geräten verschiedene Richtlinien, Profile und Apps zuzuweisen. Die Eigenschaften, die Sie einer Gerätegruppe zuweisen, haben Vorrang vor denen, die Sie einem Benutzer oder einer Benutzergruppe zuweisen. Sie können den Gerätegruppen keine Aktivierungsprofile oder Benutzerzertifikate zuweisen.

Erstellen einer Gerätegruppe

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Gruppen > Gerät**.
2. Klicken Sie auf .
3. Geben Sie einen Namen für die Gerätegruppe ein.
4. Optional wählen Sie im Abschnitt **Beschränken auf Benutzergruppen** Benutzergruppen aus, für die die Gerätegruppe angewandt wird. Wenn Sie keine Benutzergruppen auswählen, wird die Gerätegruppe für alle aktivierten Geräte angewandt.
5. Tun Sie in der ersten Dropdown-Liste im Abschnitt **Geräteabfrage** eines der folgenden Dinge:
 - Wenn Sie Geräte einbeziehen möchten, die mit allen von Ihnen definierten Attributen übereinstimmen, wählen Sie **Alle**.
 - Wenn Sie Geräte einbeziehen möchten, die mindestens mit einem der von Ihnen definierten Attribute übereinstimmen, wählen Sie **Beliebig**.
6. Legen Sie im Abschnitt **Geräteabfrage** die Parameter für die Gerätegruppe fest. Siehe [Parameter für Gerätegruppen](#).
7. Klicken Sie auf **Weiter**.
8. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Zuweisen einer IT-Richtlinie oder eines Profils zu der Gerätegruppe.	<ol style="list-style-type: none">a. Klicken Sie im Abschnitt IT-Richtlinie und -Profile auf .b. Klicken Sie auf IT-Richtlinie oder auf einen Profiltyp.c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie oder des Profils, die bzw. das Sie der Gruppe zuweisen möchten.d. Klicken Sie auf Zuweisen.

Aufgabe	Schritte
<p>Eine App und App-Gruppe der Gerätegruppe zuweisen.</p>	<ol style="list-style-type: none"> a. Klicken Sie im Abschnitt Zugewiesene Apps auf +. b. Suchen Sie nach der App, die Sie einer Gruppe zuweisen möchten, und wählen Sie diese aus. c. Klicken Sie auf Weiter. d. Führen Sie in der Dropdown-Liste Verfügbarkeit eine der folgenden Aktionen aus: <ul style="list-style-type: none"> • Damit Benutzer bei iOS- und Android-Apps die Aktionen ausführen müssen, die für Apps in dem ihnen zugewiesenen Konformitätsprofil definiert wurden, wählen Sie Erforderlich. • Damit Benutzer die App installieren müssen und Apple VPP-Apps nicht automatisch aktualisieren können, wählen Sie Erforderlich ohne Updates aus. • Um Benutzern das Installieren und Deinstallieren der App zu gestatten, wählen Sie Optional. Diese Option ist nicht für App-Gruppen verfügbar, die Android Enterprise unterstützen. • Um Benutzern das Installieren und Entfernen der App zu gestatten und zu verhindern, dass Apple VPP-Apps sich automatisch aktualisieren, wählen Sie Optional ohne Updates aus. e. Wenn Sie auf iOS-Geräten „Per App VPN“-Einstellungen einer App oder App-Gruppe zuweisen möchten, wählen Sie in der Dropdown-Liste Per App VPN die Einstellungen aus, die mit der App oder der App-Gruppe verknüpft werden sollen. f. Falls verfügbar, wählen Sie für iOS- und Android-Geräte eine App-Konfiguration aus, die der App zugewiesen werden soll. g. Wenn Sie Android Enterprise verwenden und Tracks für Apps in der Google Play-Konsole erstellt haben, wählen Sie einen Track, der der App zugewiesen werden soll. h. Klicken Sie auf Zuweisen. <p>Beachten Sie, dass Sie BlackBerry Dynamics-Apps nicht zu Gerätegruppen hinzufügen können, da Berechtigungen nur Benutzern gewährt werden können. Alle in App-Gruppen enthaltenen BlackBerry Dynamics-Apps, die Gerätegruppen hinzugefügt werden, können dem Benutzer nicht zugewiesen werden.</p> <p>Wenn Ihre Umgebung Android Enterprise unterstützt, können Sie keine Android-Apps hinzufügen, die für Gerätegruppen optional verfügbar sind. Google Play for Work kann Apps nur an Google-Benutzer-IDs zuweisen, nicht an Geräte-IDs. Wenn Sie Android-Apps hinzufügen, deren Verfügbarkeit für eine Gerätegruppe erforderlich ist, werden die Apps installiert, aber nicht in Google Play for Work aufgeführt.</p>

9. Klicken Sie auf **Speichern**.

Parameter für Gerätegruppen

Konfigurieren Sie beim Erstellen einer Gerätegruppe eine Geräteabfrage mit mindestens einer Attributeingabe. Sie können festlegen, ob ein Gerät zur Gerätegruppe gehört, wenn nur eine Attributeingabe übereinstimmt, oder ob

dazu alle Attributeingaben übereinstimmen müssen. Jede Attributeingabe enthält ein Attribut, einen Operator und einen Wert.



Attribut	Operatoren	Werte
Betreiber	<ul style="list-style-type: none"> • = • != • Beginnt mit 	Geben Sie den Namen eines Diensteanbieters an, z. B. T-Mobile oder Bell.
BlackBerry Dynamics	<ul style="list-style-type: none"> • = • != 	Wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus: <ul style="list-style-type: none"> • Deaktiviert • Aktiviert
Hersteller	<ul style="list-style-type: none"> • = • != • Beginnt mit 	Geben Sie den Namen eines Geräteherstellers an (z. B. Apple).
Modell	<ul style="list-style-type: none"> • = • != • Beginnt mit 	Geben Sie den Namen eines Gerätemodells an (z. B. iPhone 15).
OS	<ul style="list-style-type: none"> • = • != 	Wählen Sie in der Dropdown-Liste das entsprechende Betriebssystem aus.
Betriebssystemversion	<ul style="list-style-type: none"> • = • != • >= • <= 	Geben Sie die Betriebssystemversion an (z. B. 7.1.1 oder 10.3). Wenn Sie dieses Attribut verwenden, müssen Sie auch das Betriebssystemattribut festlegen.
Eigentum	<ul style="list-style-type: none"> • = • != 	Wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus: <ul style="list-style-type: none"> • Geschäftlich • Persönlich • Nicht angegeben
Aktivierungsart	<ul style="list-style-type: none"> • = • != 	Wählen Sie in der Dropdown-Liste eine Aktivierungsart aus. Die Liste enthält dieselben Aktivierungsarten, die auch für die Zuordnung Ihrer Aktivierungsprofile verfügbar sind.
Knox Workspace	<ul style="list-style-type: none"> • = • != • Beginnt mit 	Geben Sie eine Samsung Knox Workspace-Version an (z. B. 3.2.1).

Verwalten einer Gerätegruppe

Bevor Sie beginnen: [Erstellen einer Gerätegruppe](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Gruppen > Geräte**.

2. Suchen Sie die Gerätegruppe, die Sie verwalten möchten, und klicken Sie darauf.
3. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Anzeigen von Informationen über eine Gerätegruppe.	<ol style="list-style-type: none"> a. Klicken Sie auf die Registerkarte Geräte, um die Geräte anzuzeigen, die der Gerätegruppe zugewiesen wurden. b. Klicken Sie auf die Registerkarte Einstellungen, um die Benutzergruppen, Geräteabfragen, IT-Richtlinien, Profile oder Apps anzuzeigen, die der Gerätegruppe zugewiesen wurden.
Bearbeiten einer Gerätegruppe.	<ol style="list-style-type: none"> a. Klicken Sie auf . b. Nehmen Sie die Änderungen vor. c. Klicken Sie auf Speichern.
Löschen einer Gerätegruppe.	<ol style="list-style-type: none"> a. Klicken Sie auf . b. Klicken Sie auf Löschen.

Freigegebene Gerätegruppen erstellen und bearbeiten

Wenn Sie mehreren Benutzern erlauben möchten, ein iOS-Gerät gemeinsam zu nutzen, können Sie eine freigegebene Gerätegruppe erstellen. Sie können Einstellungen für die Gruppe konfigurieren, die für bestimmte Benutzer oder für alle Benutzer gelten. Wenn Sie eine freigegebene Gerätegruppe erstellen, erstellt BlackBerry UEM ein lokales Benutzerkonto, das Eigentümer der freigegebenen Gerätegruppe ist.

Um ein Gerät abzumelden, können Benutzer entweder die lokale oder die Microsoft Active Directory-Authentifizierung verwenden. Sie können die Nutzungsbestimmungen anpassen, die Benutzer akzeptieren müssen, wenn sie ein freigegebenes Gerät abmelden. Wenn das Gerät angemeldet wird, steht es dem nächsten Benutzer zur Verfügung. Freigegebene Geräte werden während des Abmeldungs- und Anmeldeprozesses von UEM verwaltet.

Diese Funktion wurde speziell für überwachte Geräte mit der folgenden Konfiguration entwickelt:

- App-Sperrmodus aktiviert
- VPP-Apps zugewiesen

Diese Funktion unterstützt keine BlackBerry Dynamics-Apps. Das gleiche BlackBerry Dynamics-Profil muss dem Benutzerkonto zugewiesen werden, das Eigentümer der freigegebenen Gerätegruppe ist, und der freigegebenen Gerätegruppe selbst. Sie müssen sicherstellen, dass die Option „Anmeldung des UEM Client bei BlackBerry Dynamics aktivieren“ im Profil nicht ausgewählt ist.

Freigegebene Gerätegruppe erstellen

Wenn Sie eine freigegebene Gerätegruppe erstellen, wird ein lokales Benutzerkonto erstellt. Dieses lokale Benutzerkonto ist Besitzer der freigegebenen Gerätegruppe.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Dedizierte Geräte > Freigegebene Gerätegruppen**.
2. Klicken Sie auf **+**.
3. Geben Sie einen Namen und eine Beschreibung für die freigegebene Gerätegruppe ein.
4. Geben Sie den Benutzernamen für die Geräteaktivierung ein.
5. Damit Benutzer die Nutzungsbedingungen akzeptieren müssen, wenn sie ein freigegebenes Gerät auschecken, wählen Sie **Nutzungsbedingungen aktivieren**, und geben die Nutzungsbedingungen an.
6. Suchen Sie für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, im Abschnitt **Berechtigte Benutzer** nach dem Benutzer, und klicken Sie darauf.

Benutzer können zu mehreren freigegebenen Gerätegruppen gehören.

7. Zum Zuweisen einer App oder App-Gruppe klicken Sie im Abschnitt **Zugewiesene Apps** auf **+** und tun Folgendes:
 - a) Suchen Sie nach der App, die Sie einer Gruppe zuweisen möchten, und wählen Sie diese aus.
 - b) Klicken Sie auf **Weiter**.
 - c) Wählen Sie für iOS- oder Android-Apps in der Dropdown-Liste **Verfügbarkeit Erforderlich** aus, damit Benutzer die Aktionen befolgen müssen, die für Apps im ihnen zugewiesenen Konformitätsprofil festgelegt sind.

Wenn die App-Gruppe Android Enterprise unterstützt, kann die Verfügbarkeit nur auf **Erforderlich** gesetzt werden.
 - d) Damit Benutzer die App installieren und deinstallieren können, wählen Sie in der Dropdown-Liste **Verfügbarkeit Optional** aus.

- e) Wenn Sie auf iOS-Geräten „Per App VPN“-Einstellungen einer App oder App-Gruppe zuweisen möchten, wählen Sie in der Dropdown-Liste **Per App VPN** die Einstellungen aus, die mit der App oder der App-Gruppe verknüpft werden sollen.
- f) Falls verfügbar, wählen Sie für iOS- und Android-Geräte eine App-Konfiguration aus, die der App zugewiesen werden soll.
- g) Wenn Sie Android Enterprise verwenden und Tracks für Apps in der Google Play-Konsole erstellt haben, wählen Sie einen Track, der der App zugewiesen werden soll.
- h) Klicken Sie auf **Zuweisen**.

Sie können keine BlackBerry Dynamics-Apps zu Gerätegruppen hinzufügen, da Berechtigungen nur Benutzern gewährt werden können. Alle in App-Gruppen enthaltenen BlackBerry Dynamics-Apps, die Gerätegruppen hinzugefügt werden, können den Benutzern nicht zugewiesen werden.

Wenn Ihre Umgebung Android Enterprise unterstützt, können Sie keine Android-Apps hinzufügen, die für Gerätegruppen optional verfügbar sind. Google Play for Work kann Apps nur an Google-Benutzer-IDs zuweisen, nicht an Geräte-IDs. Wenn Sie Android-Apps hinzufügen, deren Verfügbarkeit für eine Gerätegruppe erforderlich ist, werden die Apps installiert, aber nicht in Google Play for Work aufgeführt.

8. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- [Aktivieren eines freigegebenen Geräts](#).
- Informationen zum Ändern der freigegebenen Gerätegruppe finden Sie unter [Verwalten einer freigegebenen Gerätegruppe](#).

Aktivieren eines freigegebenen Geräts

Bevor Benutzer freigegebene Geräte abmelden können, müssen Sie diese aktivieren. Die Aktivierungsart Benutzerdatenschutz - Benutzerregistrierung wird nicht unterstützt.

Bevor Sie beginnen: Vergewissern Sie sich, dass für das BlackBerry Dynamics-Profil, das der freigegebenen Gerätegruppe zugewiesen ist, die Option „Anmeldung des UEM Client bei BlackBerry Dynamics aktivieren“ nicht ausgewählt ist. Stellen Sie sicher, dass das gleiche Profil auch dem Benutzerkonto zugewiesen ist, das Eigentümer der freigegebenen Gerätegruppe ist.




1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Dedizierte Geräte > Freigegebene Gerätegruppen**.
2. Suchen Sie nach dem Namen einer freigegebenen Gerätegruppe, und klicken Sie darauf.
3. Um die Serveradresse und Zugangsdaten zur Aktivierung des Geräts zu erhalten, klicken Sie auf **Geräteaktivierung**.
4. Befolgen Sie zum Aktivieren des Geräts die Anweisungen auf dem Bildschirm.


Wenn Sie fertig sind: Überprüfen Sie, ob das Gerät im Abschnitt **Freigegebene Geräte** angezeigt wird. Um einen Gerätenamen zu generieren, fügt BlackBerry UEM dem Gruppennamen eine Nummer hinzu. Wenn der Gruppenname zum Beispiel Demo lautet, heißt das erste Gerät, das Sie aktivieren, Demo 01.

Verwalten einer freigegebenen Gerätegruppe

Bevor Sie beginnen: [Freigegebene Gerätegruppe erstellen](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Dedizierte Geräte > Freigegebene Gerätegruppen**.
2. Suchen Sie den Namen der freigegebenen Gerätegruppe, die Sie verwalten möchten, und klicken Sie darauf.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Lassen Sie nur den Anmeldebildschirm des BlackBerry UEM Clients anzeigen, wenn das Gerät eingecheckt ist.	<ul style="list-style-type: none"> a. Klicken Sie auf . b. Aktivieren Sie das Kontrollkästchen App-Sperre von UEM-Client aktivieren. c. Klicken Sie auf Speichern.
Bearbeiten der Benutzermitgliedschaft einer freigegebenen Gerätegruppe.	<ul style="list-style-type: none"> a. Navigieren Sie zum Abschnitt Berechtigte Benutzer. b. Um der Gruppe einen Benutzer hinzuzufügen, suchen Sie nach dem Namen des Benutzers, und klicken Sie darauf. c. Um einen Benutzer aus der Gruppe zu entfernen, klicken Sie in der Spalte Aktion auf .
Zuweisen einer IT-Richtlinie oder eines Profils zu einer freigegebenen Gerätegruppe.	<p>Sie können einer freigegebenen Gerätegruppe eine IT-Richtlinie und Profile zuweisen, die entweder beim Einchecken oder beim Auschecken des Geräts durch einen Benutzer gelten. Damit unabhängig davon, ob das Gerät ein- oder ausgecheckt ist, dieselbe IT-Richtlinie bzw. dasselbe IT-Profil gilt, können Sie es für beide Zustände zuweisen. Wenn die zugewiesene IT-Richtlinie oder das zugewiesene Profil für jeden Zustand unterschiedlich ist, werden die entsprechenden Richtlinien und Profile beim Ein- und Auschecken des Geräts angewendet.</p> <ul style="list-style-type: none"> a. Klicken Sie auf der Registerkarte Ausgecheckte Einstellungen im Abschnitt Zugewiesene IT-Richtlinien und -Profile auf . b. Klicken Sie auf IT-Richtlinien oder auf einen Profiltyp. c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie bzw. des IT-Profiles, die/das Sie den Geräten beim Auschecken zuweisen möchten. d. Klicken Sie auf Zuweisen oder auf Ersetzen. e. Wiederholen Sie auf der Registerkarte Eingecheckte Einstellungen die Schritte zum Zuweisen von IT-Richtlinie und -Profilen, die für die freigegebenen Geräte gelten, wenn sie eingecheckt werden.

Aufgabe	Schritte
Zuweisen einer App zu einer freigegebenen Gerätegruppe.	<p>Sie können einer freigegebenen Gerätegruppe Apps oder App-Gruppen zuweisen, die entweder beim Einchecken oder beim Auschecken des Geräts durch einen Benutzer gelten. Damit Apps jederzeit auf dem Gerät bleiben, können Sie es beiden Status zuweisen. Zugewiesene Apps, die nur in einem Status verfügbar sind, werden entsprechend hinzugefügt oder entfernt, wenn das Gerät ein- oder ausgecheckt wird.</p> <p>Bevor Sie die folgenden Schritte ausführen, fügen Sie die App der Liste der verfügbaren Apps hinzu, oder erstellen Sie App-Gruppen.</p> <ol style="list-style-type: none"> Klicken Sie auf der Registerkarte Eingecheckte Einstellungen im Abschnitt Zugewiesene Apps auf +. Suchen Sie die App bzw. App-Gruppe, die Sie zuweisen möchten, und wählen Sie sie aus. Klicken Sie auf Weiter. Konfigurieren Sie die App-Verfügbarkeit, Per-App-VPN, App-Konfiguration, und verfolgen Sie sie nach Bedarf. Klicken Sie auf Weiter. Wählen Sie Ja, wenn Sie der App eine Lizenz zuweisen und die Lizenzeinstellungen nach Bedarf konfigurieren möchten. Wählen Sie Nein, wenn Sie keine Lizenz zuweisen möchten oder keine Lizenz haben, die Sie der App zuweisen könnten. Klicken Sie auf Zuweisen. <p>Benutzer müssen sich entsprechend der Anweisungen im VPP Ihrer Organisation auf ihrem Gerät registrieren, bevor sie vorausbezahlte Apps installieren können. Benutzer müssen diese Aufgabe ein Mal erledigen.</p> <ol style="list-style-type: none"> Wiederholen Sie auf der Registerkarte Eingecheckte Einstellungen die Schritte zum Zuweisen von Apps oder App-Gruppen, die auf dem Gerät installiert bleiben sollen, wenn das Gerät eingecheckt wird.
Ein Gerät aus einer freigegebenen Gerätegruppe entfernen.	<ol style="list-style-type: none"> Klicken Sie im Abschnitt Freigegebene Geräte in der Spalte Aktion auf X. Klicken Sie auf Nur Geschäftsdaten löschen.
Freigegebene Gerätegruppe löschen.	<ol style="list-style-type: none"> Entfernen Sie alle Geräte aus der freigegebenen Gerätegruppe. Klicken Sie auf . Klicken Sie auf Löschen.

Erstellen und Verwalten öffentlicher Gerätegruppen

Bei einem öffentlichen Gerät handelt es sich um ein Gerät, das dazu dient, einen bestimmten Zweck zu erfüllen, und daher auf bestimmte Anwendungen beschränkt ist. Diese Funktion wird für iOS- und Android Enterprise-Geräte unterstützt.

Einer öffentlichen Gerätegruppe müssen ein Profil für App-Sperrmodus und ein unterstütztes Aktivierungsprofil zugewiesen werden. Für Android Enterprise darf die Aktivierungsart nur Geschäftlicher Bereich sein (vollständig über Android Enterprise verwaltetes Gerät). Für iOS muss das Gerät ein überwacht iOS-Gerät mit MDM-Steurelementen sein.

Erstellen einer öffentlichen Gerätegruppe

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Dedizierte Geräte > Öffentliche Gerätegruppen**.
2. Klicken Sie auf **+**.
3. Geben Sie einen Namen und eine Beschreibung für die öffentliche Gerätegruppe ein.
4. Geben Sie den Benutzernamen für die Geräteaktivierung ein.
5. Zum Zuweisen einer App oder App-Gruppe zu der Gruppe klicken Sie im Abschnitt **Zugewiesene Apps** auf **+** und tun Folgendes:
 - a) Suchen Sie nach der App, die Sie einer Gruppe zuweisen möchten, und wählen Sie diese aus.
 - b) Klicken Sie auf **Weiter**.
 - c) Wählen Sie für iOS- oder Android-Apps in der Dropdown-Liste **Verfügbarkeit Erforderlich** aus, damit Benutzer die Aktionen befolgen müssen, die für Apps im ihnen zugewiesenen Konformitätsprofil festgelegt sind.

Wenn die App-Gruppe Android Enterprise unterstützt, muss die Verfügbarkeit **Erforderlich** sein.
 - d) Damit Benutzer die App installieren und deinstallieren können, wählen Sie in der Dropdown-Liste **Verfügbarkeit Optional** aus.
 - e) Wenn Sie auf iOS-Geräten „Per App VPN“-Einstellungen einer App oder App-Gruppe zuweisen möchten, wählen Sie in der Dropdown-Liste **Per App VPN** die Einstellungen aus, die mit der App oder der App-Gruppe verknüpft werden sollen.
 - f) Falls verfügbar, wählen Sie für iOS- und Android-Geräte eine App-Konfiguration aus, die der App zugewiesen werden soll.
 - g) Wenn Sie Android Enterprise verwenden und Tracks für Apps in der Google Play-Konsole erstellt haben, wählen Sie einen Track, der der App zugewiesen werden soll.

6. Klicken Sie auf **Zuweisen**.


Sie können keine BlackBerry Dynamics-Apps zu Gerätegruppen hinzufügen, da Berechtigungen nur Benutzern gewährt werden können. Alle in App-Gruppen enthaltenen BlackBerry Dynamics-Apps, die Gerätegruppen hinzugefügt werden, können den Benutzern nicht zugewiesen werden.

Wenn Sie Android Enterprise unterstützen, können Sie keine Android-Apps hinzufügen, die für Gerätegruppen optional verfügbar sind. Google Play for Work kann Apps nur an Google-Benutzer-IDs zuweisen, nicht an Geräte-IDs. Wenn Sie Android-Apps hinzufügen, deren Verfügbarkeit für eine Gerätegruppe erforderlich ist, werden die Apps installiert, aber nicht in Google Play for Work aufgeführt.

7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- [Erstellen Sie ein Profil für den App-Sperrmodus](#), und weisen Sie es der öffentlichen Gerätegruppe zu.

- [Erstellen Sie ein Aktivierungsprofil](#), und weisen Sie es einer öffentlichen Gerätegruppe zu. Die Aktivierungsart für Android Enterprise muss „Nur geschäftlicher Bereich“ sein (vollständig durch Android Enterprise verwaltetes Gerät). Die Aktivierungsart für iOS muss ein überwachtes iOS-Gerät mit MDM-Steuerelementen sein.
- [Aktivieren eines öffentlichen Geräts](#).
- Um eine öffentliche Gerätegruppe zu löschen, wählen Sie das Kontrollkästchen neben der Gruppe, die Sie löschen möchten, und klicken Sie auf .

Aktivieren eines öffentlichen Geräts

Bevor Sie beginnen: [Erstellen einer öffentlichen Gerätegruppe](#).




1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Dedizierte Geräte > Öffentliche Gerätegruppen**.
2. Suchen Sie nach dem Namen einer öffentlichen Gerätegruppe, und klicken Sie darauf.
3. Um die Serveradresse und Aktivierungszugangsdaten zur Aktivierung des Geräts zu erhalten, klicken Sie auf **Geräteaktivierung**.
4. Befolgen Sie zum Aktivieren des Geräts die Anweisungen auf dem Bildschirm.

Wenn Sie fertig sind: Überprüfen Sie, ob das aktivierte Gerät im Abschnitt **Öffentliche Geräte** angezeigt wird. Um einen Gerätenamen zu generieren, fügt BlackBerry UEM dem Gruppennamen eine Nummer hinzu. Wenn der Gruppename zum Beispiel Demo lautet, heißt das erste Gerät, das Sie aktivieren, Demo 01.

Verwalten einer öffentlichen Gerätegruppe

Bevor Sie beginnen: [Erstellen einer öffentlichen Gerätegruppe](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Dedizierte Geräte > Öffentliche Gerätegruppen**.
2. Suchen Sie nach einer öffentlichen Gerätegruppe, und klicken Sie darauf.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Einer öffentlichen Gerätegruppe eine IT-Richtlinie, ein Profil oder eine App zuweisen.	<ol style="list-style-type: none"> a. Klicken Sie im entsprechenden Abschnitt auf . b. Wählen Sie die IT-Richtlinie, das Profil oder die App aus, die Sie zuweisen möchten. Befolgen Sie die Anweisungen, und wählen Sie die entsprechenden Einstellungen aus, um die Zuweisung abzuschließen. c. Um eine IT-Richtlinie, ein Profil oder eine App zu entfernen, klicken Sie neben der Eigenschaft, die Sie löschen möchten, auf .
Gerät aus einer öffentlichen Gerätegruppe entfernen.	Klicken Sie im Abschnitt Öffentliche Geräte in der Spalte Aktion für das Gerät auf  .

Erstellen und Verwalten von Gruppen gemeinsam genutzter iPads

Wenn Sie eine Gruppe gemeinsam genutzter iPads erstellen, können sich Benutzer mit ihrer verwalteten Apple-ID bei einer Gruppe gemeinsam genutzter iPads anmelden, sodass sie gängige Apps und Lesezeichen verwenden und gleichzeitig separate Benutzerdetails beibehalten und synchronisieren können.

Beachten Sie die folgenden Anforderungen:

- Das iPad-Gerät muss ein überwachtes, MDM-registriertes Gerät sein.
- Das iPad-Gerät muss beim DEP registriert sein.
- Das iPad-Gerät muss eine unterstützte iPadOS-Version verwenden.

Diese Funktion unterstützt keine BlackBerry Dynamics-Apps. Sie müssen sicherstellen, dass die Option „Anmeldung des UEM Client bei BlackBerry Dynamics aktivieren“ im BlackBerry Dynamics-Profil nicht ausgewählt ist.

Erstellen einer Gruppe gemeinsam genutzter iPads

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Dedizierte Geräte > Gruppen gemeinsam genutzter iPads**.
2. Klicken Sie auf **+**.
3. Geben Sie einen Namen und eine Beschreibung für die gemeinsam genutzte iPad-Gruppe ein.
4. Geben Sie den Benutzernamen für die Geräteaktivierung ein.
5. Zum Zuweisen einer App oder App-Gruppe zu der Gruppe klicken Sie im Abschnitt **Zugewiesene Apps** auf **+** und tun Folgendes:
 - a) Suchen Sie nach der App, die Sie einer Gruppe zuweisen möchten, und klicken Sie darauf.
 - b) Klicken Sie auf **Weiter**.
 - c) Damit Benutzer die für Apps in ihrem zugewiesenen Konformitätsprofil definierten Aktionen ausführen müssen, wählen Sie in der Dropdown-Liste **Verfügbarkeit Erforderlich** oder **Erforderlich ohne Updates** aus.
 - d) Wenn Sie der Gruppe Per-App-VPN-Einstellungen zuweisen möchten, wählen Sie in der Dropdown-Liste **Per App VPN** die Einstellungen aus, die mit der Gruppe verknüpft werden sollen.
 - e) Wählen Sie falls verfügbar die Konfiguration aus, die der App zugewiesen werden soll.
 - f) Klicken Sie auf **Zuweisen**.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Optional [Erstellen eines Profils für ein gemeinsam genutztes iPad](#).
- [Aktivieren eines gemeinsam genutzten iPad-Geräts](#).
- Informationen zum Ändern einer Gruppe gemeinsam genutzter iPads finden Sie unter [Verwalten einer Gruppe gemeinsam genutzter iPads](#).

Erstellen eines Profils für ein gemeinsam genutztes iPad

Optional können Sie ein Profil für ein gemeinsam genutztes iPad erstellen und zuweisen, um zu konfigurieren, wie Benutzer ein gemeinsam genutztes iPad verwenden können.

Bevor Sie beginnen: [Erstellen einer Gruppe gemeinsam genutzter iPads](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Richtlinien und Profile > Richtlinie > Gemeinsam genutztes iPad**.
2. Klicken Sie auf **+**.
3. Geben Sie einen Namen und eine Beschreibung für das gemeinsame iPad-Profil ein.
4. Geben Sie im Feld **Kontingentsgröße** die Größe des Kontingents für jeden Benutzer auf dem gemeinsam genutzten Gerät in MB an. Diese Einstellung hat Vorrang vor der Einstellung unter „Residente Benutzer“.
5. Geben Sie im Feld **Residente Benutzer** die Anzahl der Benutzer an, für die der verbleibende Gerätespeicher partitioniert werden soll.
6. Wenn das Gerät nur den Gastmodus verwenden soll, wählen Sie die Option **Nur temporäre Sitzung**.
7. Geben Sie im Feld **Zeitüberschreitung für temporäre Sitzung** das Zeitlimit für temporäre Sitzungen in Sekunden an.
8. Geben Sie im Feld **Zeitüberschreitung für Benutzersitzung** das Zeitlimit für eine reguläre Sitzung in Sekunden an.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Weisen Sie das Profil der Gruppe gemeinsam genutzter iPad s zu.
- [Aktivieren eines gemeinsam genutzten iPad-Geräts](#).

Aktivieren eines gemeinsam genutzten iPad-Geräts

Bevor Sie beginnen:

- [Erstellen einer Gruppe gemeinsam genutzter iPad s](#). Optional [Erstellen eines Profils für ein gemeinsam genutztes iPad](#).
 - Erstellen Sie eine DEP-Konfiguration, wobei die Option „Modus für gemeinsam genutzte iPads aktivieren“ ausgewählt ist, und weisen Sie sie einem für DEP aktivierten iPad-Gerät zu.
 - Löschen Sie das iPad-Gerät.
 - Vergewissern Sie sich, dass für das BlackBerry Dynamics-Profil, das der Gruppe gemeinsam genutzter iPads zugewiesen ist, die Option **Anmeldung des UEM Client bei BlackBerry Dynamics aktivieren** nicht ausgewählt ist. Stellen Sie sicher, dass das gleiche Profil auch dem Benutzerkonto zugewiesen ist, das Eigentümer der Gruppe gemeinsam genutzter iPads ist.
1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Dedizierte Geräte > Gruppen gemeinsam genutzter iPads**.
 2. Suchen Sie nach dem Namen der Gruppe gemeinsam genutzter iPads, und klicken Sie darauf.
 3. Um die Aktivierungszugangsdaten zur Aktivierung des Geräts zu erhalten, klicken Sie auf **Geräteaktivierung**.
 4. Befolgen Sie zum Aktivieren des Geräts die Anweisungen zur Geräteaktivierung auf dem Bildschirm.

Wenn Sie fertig sind: Um ein Gerät aus einer Gruppe gemeinsam genutzter iPads zu entfernen, klicken Sie auf den Namen der Gruppe, aus der Sie das Gerät entfernen möchten. Klicken Sie auf dem Bildschirm **Gerätedetails** auf **Gerät entfernen** oder **Alle Gerätedaten löschen**.

Verwalten einer Gruppe gemeinsam genutzter iPad s

Bevor Sie beginnen: [Erstellen einer Gruppe gemeinsam genutzter iPad s](#).

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Dedizierte Geräte > Gruppen gemeinsam genutzter iPads**.

2. Suchen Sie nach einer Gruppe gemeinsam genutzter iPads, und klicken Sie sie an.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
<p>Einer Gruppe gemeinsam genutzter iPads eine IT-Richtlinie oder ein Profil zuweisen.</p>	<ol style="list-style-type: none"> a. Klicken Sie im Abschnitt Zugewiesene IT-Richtlinien und -Profile auf +. b. Klicken Sie auf IT-Richtlinien oder auf einen Profiltyp. c. Klicken Sie in der Dropdown-Liste auf den Namen der IT-Richtlinie oder des Profils, die bzw. das Sie zuweisen möchten. d. Klicken Sie auf Zuweisen oder auf Ersetzen.
<p>Einer Gruppe gemeinsam genutzter iPads eine App zuweisen.</p>	<p>Sie können keine BlackBerry Dynamics-Apps zu Gruppen gemeinsam genutzter iPads hinzufügen, da Berechtigungen nur Benutzern gewährt werden können. Alle in App-Gruppen enthaltenen BlackBerry Dynamics-Apps, die Gruppen gemeinsam genutzter iPads hinzugefügt werden, werden Benutzern nicht zugewiesen.</p> <p>Nur Apps aus dem VPP-Store oder interne iOS-Apps sowie iOS-App-Shortcuts werden unterstützt. Nicht aus dem VPP-Store stammende Apps werden nicht unterstützt.</p> <ol style="list-style-type: none"> a. Klicken Sie im Abschnitt Zugewiesene Apps auf +. b. Suchen Sie die App bzw. App-Gruppe, die Sie zuweisen möchten, und wählen Sie sie aus. c. Klicken Sie auf Weiter. d. Klicken Sie erneut auf Weiter. e. Weisen Sie dem Gerät für jede App eine VPP-App-Lizenz zu. f. Klicken Sie auf Zuweisen.

Verwalten von Chrome OS-Geräten in BlackBerry UEM

Sie können Chrome OS in die BlackBerry UEM-Verwaltungskonsolle integrieren, um die Fähigkeit zu erweitern, einige administrative Aufgaben in UEM auszuführen. Sie registrieren weiterhin Chrome OS-Geräte und führen einige administrative Aufgaben in Ihrer Google-Admin-Konsole aus. Wenn Sie Chrome OS in UEM integrieren, sortiert es die Organisationseinheiten aus der Google-Admin-Konsole in UEM-Organisationseinheitengruppen. Wenn eine Änderung an einer Organisationseinheit, einem Benutzer oder einem Gerät in der Google-Domäne vorgenommen wird, aktualisiert UEM die Datenbank entsprechend.

Weitere Informationen zum Konfigurieren von UEM zur Unterstützung von Chrome OS-Geräten finden Sie unter [Erweitern der Verwaltung von Chrome OS-Geräten auf BlackBerry UEM](#).

Chrome OS-Geräte verwalten

Bevor Sie beginnen: [Erweitern der Verwaltung von Chrome OS-Geräten auf BlackBerry UEM](#).

Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Anzeigen von Organisationseinheiten für Chrome OS-Benutzer.	<ol style="list-style-type: none">Klicken Sie in der Menüleiste der Verwaltungskonsolle auf Benutzer > Alle Benutzer.Suchen Sie nach einem Chrome OS-Benutzer, und klicken Sie ihn an.Die Organisationseinheit, zu der der Benutzer gehört, wird oben auf der Seite angezeigt. Sie können auf den Namen der Organisationseinheit klicken, um die aktuellen Einstellungen anzuzeigen.
Bearbeiten einer Organisationseinheit.	<p>Die Informationen, die für die Organisationseinheiten angezeigt werden, replizieren die in der Google-Admin-Konsole vorgenommene Konfiguration. Sie können bestimmte Felder in einer Organisationseinheit bearbeiten, viele der Einstellungen können jedoch nur in der Google-Admin-Konsole geändert werden.</p> <ol style="list-style-type: none">Klicken Sie in der Menüleiste der Verwaltungskonsolle auf Gruppen > Organisationseinheit.Klicken Sie auf die Organisationseinheit, die Sie bearbeiten möchten.Nehmen Sie die notwendigen Änderungen vor.Klicken Sie auf Speichern.

Aufgabe	Schritte
Befehle an Chrome OS-Geräte senden.	<p>a. Klicken Sie in der Menüleiste der Verwaltungskonsole auf Benutzer > Alle Benutzer.</p> <p>b. Suchen Sie nach einem Chrome OS-Benutzer, und klicken Sie ihn an.</p> <p>c. Führen Sie im Abschnitt Gerät verwalten einen der folgenden Befehle aus:</p> <ul style="list-style-type: none"> • Anzeigen des Geräteberichts: Mit diesem Befehl werden detaillierte Informationen über das Gerät angezeigt. • Anzeigen der Geräteaktionen: Mit diesem Befehl werden alle Aktionen angezeigt, die gerade auf dem Gerät durchgeführt werden. • Gerät deaktivieren: Mit diesem Befehl wird das Gerät deaktiviert. Beachten Sie, dass der Benutzer das Gerät nicht erneut aktivieren kann, nachdem es von einem Administrator deaktiviert wurde. • Gerät aktivieren: Mit diesem Befehl wird das Gerät aktiviert. • Alle Gerätedaten löschen: Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht und das Gerät auf die Standardeinstellungen zurückgesetzt. • Nur geschäftliche Daten löschen: Mit diesem Befehl werden geschäftliche Daten gelöscht und die Bereitstellung des Geräts wird aufgehoben. • Gerät entfernen: Mit diesem Befehl wird die Bereitstellung des Geräts aufgehoben.

Einrichtung der BlackBerry UEM Self-Service

BlackBerry UEM Self-Service ist eine webbasierte Anwendung, die es Gerätebenutzern ermöglicht, Verwaltungsaufgaben wie das Erstellen von Aktivierungskennwörtern, das Sperren von Geräten per Fernzugriff oder das Löschen von Daten von Geräten durchzuführen. Um UEM Self-Service zu verwenden, müssen Sie den Benutzern die Webadresse und die Anmeldeinformationen bereitstellen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Self-Service > Self-Service-Einstellungen**.
2. Vergewissern Sie sich, dass das Kontrollkästchen **Benutzern den Zugriff auf die Self-Service-Konsole gestatten** aktiviert ist.
3. Geben Sie an, wie viel Zeit ein Benutzer hat, um ein Gerät zu aktivieren, bevor das Aktivierungskennwort abläuft.
4. Geben Sie die Mindestanzahl von Zeichen an, die für ein Aktivierungskennwort erforderlich sind.
5. Wählen Sie in der Dropdown-Liste **Mindestkomplexität des Kennworts** die für Aktivierungskennwörter erforderliche Komplexität aus.
6. Um automatisch eine Aktivierungs-E-Mail an Benutzer zu senden, wenn sie ein Aktivierungskennwort in UEM Self-Service erstellen, aktivieren Sie das Kontrollkästchen **Aktivierungs-E-Mail senden**. Sie können die standardmäßige Aktivierungs-E-Mail-Vorlage verwenden oder eine andere Vorlage aus der Dropdown-Liste auswählen.
7. Um dem Benutzer jedes Mal, wenn er sich bei UEM Self-Service anmeldet, eine Anmeldebenachrichtigungs-E-Mail zu senden, aktivieren Sie das Kontrollkästchen **Benachrichtigung für Self-Service-Anmeldung senden**.
8. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Geben Sie die Webadresse für BlackBerry UEM Self-Service und die Anmeldeinformationen für die Benutzer an.
- Informationen zum Erstellen und Verwalten von Benutzerrollen für UEM Self-Service, siehe [Verwalten von Benutzerrollen für BlackBerry UEM Self-Service](#).

Verwalten von Benutzerrollen für BlackBerry UEM Self-Service

Mithilfe von Benutzerrollen können Sie angeben, welche Funktionen in BlackBerry UEM Self-Service für Benutzer verfügbar sein sollen. BlackBerry UEM umfasst eine vorkonfigurierte Standard-Benutzerrolle. Die Standard-Benutzerrolle ist so eingerichtet, dass sie alle UEM Self-Service-Funktionen zulässt, und sie wird der Gruppe „Alle Benutzer“ zugeordnet.

Hinweis: Das Umbenennen, Löschen oder Entfernen der Standard-Benutzerrolle aus der Gruppe „Alle Benutzer“ kann zu Problemen mit geschäftlichen Apps auf iOS-Geräten führen.

Wenn Sie bestimmte Funktionen für Benutzer sperren möchten, können Sie neue Benutzerrollen erstellen oder eine bestehende Benutzerrolle bearbeiten. Sie können Benutzerrollen Gruppen oder den Benutzern direkt zuweisen.

Jedem Benutzer wird nur eine Rolle zugewiesen. Eine Rolle, die einem Benutzerkonto direkt zugewiesen wird, hat Vorrang vor einer indirekt von einer Benutzergruppe zugewiesenen Rolle. Wenn ein Benutzer Mitglied mehrerer Benutzergruppen mit verschiedenen Rollen ist, weist UEM die Rolle mit der höchsten Rangordnung zu.


BlackBerry UEM Self-Service-Funktionen

Funktion	Beschreibung
Ein Aktivierungskennwort festlegen	Benutzer können ein Kennwort erstellen, mit dem sie ihre Geräte mit BlackBerry UEM aktivieren können. Sie können die Standard-Ablaufzeit für Kennwörter und die erforderliche Komplexität des Kennworts unter „Einstellungen > Self-Service > Self-Service-Einstellungen“ konfigurieren.
Zugriffsschlüssel festlegen	Benutzer können Zugriffsschlüssel für die Aktivierung von BlackBerry Dynamics-Apps erstellen.
Nur geschäftliche Daten löschen	Benutzer können den Befehl „Nur geschäftliche Daten löschen“ an ein Gerät senden. Der Befehl löscht geschäftliche Daten, z. B. IT-Richtlinien, Profile, Apps und Zertifikate.
Alle Gerätedaten löschen	Benutzer können den Befehl „Alle Gerätedaten löschen“ an ein Gerät senden. Mit diesem Befehl werden alle Benutzerinformationen und App-Daten gelöscht, die auf dem Gerät gespeichert sind, einschließlich der im geschäftlichen Bereich. Er setzt das Gerät auf die werkseitigen Standardeinstellungen zurück und löscht das Gerät aus UEM.
Standort des Geräts bestimmen	Benutzer können den Standort ihrer iOS- oder Android-Geräte auf einer Karte anzeigen lassen. Diese Funktion erfordert, dass dem Benutzer ein Profil für die Standortbestimmung zugewiesen wurde. Weitere Informationen finden Sie unter Verwenden von Standortdiensten auf Geräten .
Benutzerzertifikate verwalten	Benutzer können Benutzerzertifikate für ihre Geräte hochladen. Sie haben die Möglichkeit, Benutzern Anweisungen zu den benötigten Zertifikaten und zum Ort, von dem sie die Zertifikate hochladen können, bereitzustellen.

Funktion	Beschreibung
BlackBerry Dynamics-Apps sperren und entsperren	Wenn Benutzergeräte für die Nutzung von BlackBerry Dynamics aktiviert wurden, können Benutzer die auf ihren Geräten installierten BlackBerry Dynamics-Apps sperren und Entsperrschlüssel zum Entsperren der Apps erzeugen. Wenn eine App vom Benutzer gesperrt wird, kann sie nicht mehr geöffnet werden.
BlackBerry Dynamics-Appdaten löschen	Wenn Benutzergeräte für die Nutzung von BlackBerry Dynamics aktiviert wurden, können Benutzer alle Daten einer auf ihrem Gerät installierten BlackBerry Dynamics-App löschen. Mit diesem Befehl werden alle von der App gespeicherten Daten entfernt, die App selbst wird jedoch nicht gelöscht.

Erstellen einer Benutzerrolle für UEM Self-Service

Sie können eine benutzerdefinierte Rolle erstellen und diese Benutzern oder Gruppen zuweisen, um damit die Funktionalität festzulegen, die Benutzer in BlackBerry UEM Self-Service nutzen können.





1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Self-Service > Benutzerrollen**.
2. Klicken Sie auf .
3. Geben Sie einen Namen und eine Beschreibung für die Benutzerrolle ein.
4. Um Berechtigungen einer anderen Rolle zu kopieren, klicken Sie auf eine Rolle in der Dropdown-Liste **Berechtigungen von Rolle übernommen**.
5. Wählen Sie die Funktionen aus, die für die Benutzerrolle verfügbar sein sollen.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Ordnen Sie die Benutzerrollen entsprechend, und speichern Sie Ihre Änderungen.
- Weisen Sie Benutzerrollen Benutzergruppen (**Gruppen > Suchen Sie nach einer Gruppe, und klicken Sie darauf > Verwaltete Geräte**) oder einzelnen Benutzern (**Benutzer > Verwaltete Geräte > Suchen Sie nach einem Benutzer, und klicken Sie darauf > Direkte Rollenzuweisung**) zu.

Anpassen der Benutzerliste

1. Klicken Sie in der Menüleiste der Verwaltungskonsolle auf **Benutzer > Verwaltete Geräte**.
2. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Stellen Sie die standardmäßige oder erweiterte Ansicht ein.	Klicken Sie in der oberen rechten Ecke auf Standard oder Erweitert . In größeren Umgebungen kann die Anzeige der erweiterten Ansicht mehr Zeit in Anspruch nehmen als dies bei der Standardansicht der Fall ist.
Auswählen der Informationen, die in der Benutzerliste angezeigt werden.	<p>a.  .</p> <p>Klicken Sie oben in der Benutzerliste auf  .</p> <p>b. Wählen Sie die Spalten, die Sie ein- oder ausschließen möchten.</p> <p>Um die Benutzerliste nach einer Spalte zu filtern, klicken Sie auf die Spaltenüberschrift.</p> <p>Um die Spalten neu anzuordnen, klicken und ziehen Sie eine Spaltenüberschrift.</p>
Filtern der Benutzerliste.	<p>Falls Sie die Mehrfachauswahl einschalten, können Sie mehrere Filter auswählen, bevor Sie diese anwenden, und Sie können für jede Kategorie mehrere Filter auswählen. Falls Mehrfachauswahl ausgeschaltet ist, wird der jeweilige Filter bei Auswahl angewendet, und Sie können jeweils nur einen Filter für eine Kategorie auswählen.</p> <p>a. Klicken Sie auf , um die Mehrfachauswahl ein- oder auszuschalten.</p> <p>b. Erweitern Sie eine oder mehrere Kategorien unter Filter. Jede Kategorie enthält nur Filter, die Ergebnisse anzeigen und jeder Filter gibt die Anzahl der Ergebnisse an, die angezeigt werden, wenn Sie den Filter anwenden.</p> <p>c. Wählen Sie die Filter aus, die Sie anwenden möchten.</p>
Exportieren der Benutzerliste in eine .csv-Datei.	<p>Wenn Sie die Benutzerliste exportieren, enthält die Datei alle Spalten, die derzeit angezeigt werden.</p> <p>a. Wählen Sie die Benutzerkonten aus, die Sie beim Export einschließen wollen. Sie können das Kontrollkästchen oben in der Benutzerliste aktivieren, um alle Benutzer auszuwählen.</p> <p>b. Klicken Sie auf , und speichern Sie die Datei.</p>

Aufgabe	Schritte
Ändern der Kennzeichnung für den Geräteeigentümer.	<p>Jedes aktivierte Gerät verfügt über eine Kennzeichnung, die angibt, ob das Gerät im Besitz des Unternehmens oder Benutzers ist oder ob der Eigentümer nicht angegeben wurde. Der Standardwert wird vom im Aktivierungsprofil angegebenen Wert für den Geräteeigentümer übernommen. Sie können die Benutzerliste nach der Kennzeichnung für den Geräteeigentümer filtern. Führen Sie die folgenden Schritte aus, um die Kennzeichnung für den Geräteeigentümer für einen bestimmten Benutzer zu ändern. Wenn Sie die Kennzeichnung für mehrere Benutzer ändern möchten, können Sie einen Stapelbefehl senden.</p> <ol style="list-style-type: none"><li data-bbox="630 604 1474 667">a. Suchen Sie nach dem Namen eines Benutzerkontos, und klicken Sie darauf.<li data-bbox="630 674 1474 737">b. Klicken Sie im Bereich Aktivierte Geräte neben der Einstellung „Eigentümer“ auf Bearbeiten.<li data-bbox="630 743 1474 806">c. Legen Sie die entsprechende Kennzeichnung für den Geräteeigentümer fest.<li data-bbox="630 812 1474 846">d. Klicken Sie auf Speichern.

Rechtliche Hinweise

©2024 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

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.

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

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

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

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

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

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

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

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE PASSAGE IN DIESEM DOKUMENT IST DAZU VORGESEHEN, BELIEBIGE SCHRIFTLICHE VEREINBARUNGEN ODER GARANTIE, 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