BlackBerry UEM

Konfiguration

12.12

Inhalt

Erstmalige Konfiguration von BlackBerry UEM

In der folgenden Tabelle sind die ursprünglichen Konfigurationsaufgaben, die in diesem Handbuch besprochen werden, zusammengefasst. Verwenden Sie diese Tabelle, um zu bestimmen, welche Konfigurationsaufgaben Sie abschließen sollten. Nach Abschluss der entsprechenden Aufgaben können Sie Administratoren einrichten, Benutzer und Gruppen erstellen und verwalten, Gerätesteuerungen einrichten und Geräte aktivieren.

Aufgabe	Beschreibung
Standardzertifikate durch vertrauenswürdige Zertifikate ersetzen	Sie können die selbstsignierten Standardzertifikate ersetzen, die von BlackBerry UEM verwendet werden, um die Kommunikation zwischen verschiedenen UEM-Komponenten und Geräten zu authentifizieren.
Konfigurieren von BlackBerry UEM zum Senden von Daten über einen Proxyserver	Sie können BlackBerry UEM so konfigurieren, dass Daten zuerst über einen TCP-Proxyserver oder eine Instanz des BlackBerry Router gesendet werden, bevor sie die BlackBerry Infrastructure erreichen. Sie können BlackBerry UEM zudem so konfigurieren, dass Daten zuerst über einen HTTP-Proxy gesendet werden, bevor sie die BlackBerry Dynamics NOC erreichen.
Konfigurieren von Verbindungen über interne Proxyserver	Wenn Ihr Unternehmen einen Proxyserver für Verbindungen zwischen den Servern in Ihrem Netzwerk nutzt, müssen Sie die serverseitigen Proxyeinstellungen möglicherweise so konfigurieren, dass BlackBerry UEM Core mit Remote-Instanzen der Verwaltungskonsole kommunizieren kann.
Herstellung einer Verbindung zwischen BlackBerry UEM und Unternehmensverzeichnissen	Sie können BlackBerry UEM mit Unternehmensverzeichnissen verbinden, z. B. Microsoft Active Directory- oder ein LDAP-Verzeichnis, sodass BlackBerry UEM zum Erstellen von Benutzerkonten auf Benutzerdaten zugreifen kann.
Herstellen einer Verbindung zwischen BlackBerry UEM und einem SMTP-Server	Wenn Sie möchten, dass BlackBerry UEM Aktivierungs-E-Mails und andere Benachrichtigungen an Benutzer sendet, müssen Sie die Einstellungen für den SMTP-Server festlegen, den BlackBerry UEM verwenden kann.
Datenbankspiegelung konfigurieren	Um den Datenbankdienst und die Datenintegrität aufrechtzuerhalten, wenn Probleme mit der BlackBerry UEM-Datenbank auftreten, können Sie eine Failover-Datenbank als Sicherung der Prinzipaldatenbank installieren und konfigurieren.
Verbinden von BlackBerry UEM mit Microsoft Azure	Wenn Sie BlackBerry UEM zum Bereitstellen von iOS- und Android-Apps verwenden möchten, die von Microsoft Intune verwaltet werden, oder wenn Sie Windows 10-Apps in BlackBerry UEM verwalten möchten, verbinden Sie BlackBerry UEM mit Microsoft Azure.
APNs-Zertifikat abrufen und registrieren	Wenn Sie iOS- oder macOS-Geräte verwalten und Daten an diese Geräte senden möchten, müssen Sie eine signierte CSR-Datei von BlackBerry abrufen, mit dieser ein APNs-Zertifikat von Apple abrufen und das APNs-Zertifikat bei der BlackBerry UEM-Domäne registrieren.
Konfigurieren von BlackBerry UEM für das Programm zur Geräteregistrierung von Apple	Wenn Sie die BlackBerry UEM-Verwaltungskonsole zum Verwalten der iOS-Geräte verwenden möchten, die von Ihrem Unternehmen von Apple für das Programm zur Geräteregistrierung (DEP) erworben wurden, müssen Sie diese Funktion konfigurieren.

Aufgabe	Beschreibung
Konfigurieren von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten	Zur Unterstützung von Android Enterprise-Geräten müssen Sie Ihre G Suite- bzw. Google Cloud-Domäne zur Unterstützung der Verwaltung mobiler Geräte von Drittanbietern und BlackBerry UEM für die Kommunikation mit Ihrer G Suite- bzw. Google Cloud-Domäne konfigurieren.
Netzwerk zur Vereinfachung von Windows 10-Aktivierungen konfigurieren	Sie können diesen Vorgang zur Aktivierung von Windows 10-Geräten vereinfachen, indem Sie Konfigurationsänderungen an Ihrem Netzwerk vornehmen, sodass Benutzer keine Serveradresse mehr eingeben müssen.
Migrieren von Benutzern, Geräten, Gruppen und anderen Daten aus einem Quellserver	Über die Verwaltungskonsole können Sie Benutzer, Geräte, Gruppen und andere Daten aus einer lokalen BlackBerry UEM oder Good Control (eigenständig) migrieren.
BlackBerry Dynamics-Einstellungen konfigurieren	Sie können Einstellungen konfigurieren, die speziell für BlackBerry Proxy- und BlackBerry Dynamics-Apps gelten.
Integrieren von BlackBerry UEM mit Cisco ISE	Sie können eine Verbindung zwischen Cisco ISE und BlackBerry UEM herstellen, damit Cisco ISE Gerätedaten aus BlackBerry UEM abrufen und die Steuerung des Netzwerkzugriffs durchsetzen kann.

Konfigurationsschritte für die Verwaltung von BlackBerry OS-Geräten

Wenn die BlackBerry UEM-Domäne Ihres Unternehmens Geräte mit BlackBerry OS (Version 5.0 bis 7.1) unterstützt, können Sie die Verwaltung von BlackBerry OS-Geräten individualisieren. Wenn Sie ein Upgrade von BES5 auf BlackBerry UEM durchgeführt haben, bleiben die Konfigurationen der BES5-Komponenten nach dem Upgrade intakt, sodass keine weiteren Konfigurationsschritte erforderlich sind.

Anweisungen zu den einzelnen Aufgaben in der Tabelle finden Sie in der BES5-Dokumentation.

Durchzuführende Aufgabe	Ressource
Festlegen, welcher Dienst Kalenderdaten verwaltet Standardmäßig übernimmt Microsoft Exchange Web Services die Verwaltung von Kalenderdaten für BlackBerry OS-Geräte. Wenn ein Benutzer nicht die Berechtigung zum Verwenden dieses Dienstes aufweist, werden die Kalenderdaten des Benutzers mithilfe von MAPI- und CDO-Bibliotheken verwaltet. Sie können entscheiden, ob Kalenderdaten ausschließlich über Microsoft Exchange Web Services oder ausschließlich über MAPI- und CDO-Bibliotheken verwaltet werden sollen.	*Installations- und Konfigurationshandbuch* • Aufgaben nach der Installation: Konfigurieren des BlackBerry Enterprise Server für die Verwendung von Microsoft Exchange Web Services
Verwenden des SNMP-Diensts zur Überwachung der Komponenten, die BlackBerry OS-Geräte verwalten	*Installations- und Konfigurationshandbuch* • Aufgaben nach der Installation: Konfigurieren eines Computers für die Überwachung

Durchzuführende Aufgabe	Ressource
Mithilfe einer Enterprise Service Policy steuern, welche BlackBerry OS-Geräte auf BlackBerry UEM zugreifen können.	*Administratorhandbuch für* • Konfigurieren von Sicherheitsoptionen: Verwalten des Zugriffs von Geräten auf den BlackBerry Enterprise Server
Konfigurieren von BlackBerry MDS Connection Service, BlackBerry Collaboration Service und BlackBerry Administration Service, sodass Daten über einen Proxy-Server gesendet werden.	*Administratorhandbuch für* • Konfiguration der BlackBerry Enterprise Server-Umgebung
Konfigurieren hoher Verfügbarkeit für Komponenten, die BlackBerry OS-Geräte verwalten.	*Administratorhandbuch für* • Konfigurieren hoher Verfügbarkeit für BlackBerry Enterprise Server • Konfigurieren hoher Verfügbarkeit für BlackBerry Enterprise Server-Komponenten • Konfigurieren hoher Verfügbarkeit für BlackBerry Configuration Database
Ändern der Handhabung von Push-Daten und des benutzerseitigen Zugriffs auf Webinhalte durch BlackBerry MDS Connection Service für BlackBerry OS-Geräte	*Administratorhandbuch für* • Konfigurieren des Zugriffs von Benutzern auf Unternehmensanwendungen und Webinhalte • Verwalten des Zugriffs von Benutzern auf Unternehmensanwendungen und Webinhalte
Verwenden von Erweiterungs-Plug-Ins für die Verarbeitung von und Änderungen an E-Mail-Nachrichten und Anlagen auf BlackBerry OS-Geräten.	*Administratorhandbuch für* • Einrichten der Nachrichtenumgebung: Erweiterungs-Plug-Ins für die Verarbeitung von Nachrichten
Zulassen, dass BlackBerry OS-Geräte Zertifikate für die Authentifizierung bei Anwendungen oder Netzwerken anmelden	*Administratorhandbuch für* • Konfigurieren von BlackBerry-Geräten zur Zertifikatregistrierung über das Drahtlosnetzwerk
Zulassen, dass Benutzer von BlackBerry OS-Geräten Selbsthilfeaufgaben mithilfe des BlackBerry Web Desktop Manager ausführen.	*Administratorhandbuch für* • Bereitstellen von BlackBerry Web Desktop Manager für Benutzer • Konfigurieren von BlackBerry Web Desktop Manager
Ändern, wie Apps, OS-Updates und Einstellungen an BlackBerry OS-Geräte gesendet werden.	*Administratorhandbuch für* • Handhabung der Übermittlung von BlackBerry Java Applications, BlackBerry Device Software und Geräteeinstellungen an BlackBerry-Geräte

Durchzuführende Aufgabe	Ressource
Ändern der Synchronisierung von Terminplanerdaten für Benutzer von BlackBerry OS-Geräten.	*Administratorhandbuch für* • Verwalten der Synchronisierung von Terminplanerdaten
Ändern der Nachrichtenkonfiguration und der Anlagenunterstützung für Komponenten, die BlackBerry OS-Geräte verwalten.	*Administratorhandbuch für* • Verwalten der Nachrichtenumgebung Ihres Unternehmens und Unterstützung von Anlagen
Ändern verschiedener Protokolldateieinstellungen, z. B. Speicherort, Detailebene und Maximalgröße	*Administratorhandbuch für* • BlackBerry Enterprise Server-Protokolldateien
Überprüfen und ggf. Ändern der Ports, die von Komponenten verwendet werden, die BlackBerry OS-Geräte verwalten.	*Administratorhandbuch für* • BlackBerry Enterprise Solution-Verbindungstypen und -Portnummern

Zur Konfiguration von BlackBerry UEM erforderliche Administratorberechtigungen

Wenn Sie die in diesem Handbuch beschriebenen Konfigurationsschritte ausführen, melden Sie sich mit dem während der Installation von BlackBerry UEM erstellten Administratorkonto bei der Verwaltungskonsole an. Wenn mehrere Personen Konfigurationsaufgaben durchführen sollen, können Sie zusätzliche Administratorkonten erstellen. Weitere Informationen zum Erstellen von Administratorkonten finden Sie in der Dokumentation für Administratoren.

Wenn Sie zusätzliche Administratorkonten für die Konfiguration von BlackBerry UEM erstellen, müssen Sie den Konten die Sicherheitsadministratorrolle zuweisen. Die Standard-Sicherheitsadministratorrolle weist die erforderlichen Berechtigungen für die Ausführung aller Konfigurationsaufgaben auf.

Abrufen und Aktivieren von Lizenzen

Zum Aktivieren von Geräten müssen Sie die erforderlichen Lizenzen erwerben. Sie sollten die Lizenzen beziehen, bevor Sie die Konfigurationsanweisungen in dieser Anleitung befolgen und bevor Sie Benutzerkonten hinzufügen.

Weitere Informationen zu den Lizenzierungsoptionen und den Funktionen und Produkten, die von den verschiedenen Lizenztypen unterstützt werden, finden Sie in der Dokumentation zur Lizenzierung.

Ändern eines BlackBerry UEM-Zertifikats

Wenn Sie BlackBerry UEM installieren, generiert die Setupanwendung mehrere selbstsignierte Zertifikate, die für die Authentifizierung der Kommunikation zwischen verschiedenen UEM-Komponenten und mit Geräten verwendet werden. Sie können die Zertifikate ändern, wenn die Sicherheitsrichtlinien Ihrer Organisation vorschreiben, dass Zertifikate von der Zertifizierungsstelle Ihrer Organisation signiert werden, oder wenn Sie Zertifikate verwenden möchten, die von einer Zertifizierungsstelle ausgegeben wurden, denen Geräte und Browser bereits vertrauen.

Hinweis: Wenn Probleme auftreten, wenn Sie ein Zertifikat ändern, kann die Kommunikation zwischen den UEM-Komponenten und zwischen UEM und Geräten gestört werden. Wenn Sie Zertifikate ändern wollen, planen und testen Sie die Änderung sorgfältig.

Sie können folgende Zertifikate ändern:

Zertifikat	Beschreibung
SSL-Zertifikat für Konsolen und BlackBerry Web Services	Ein SSL-Zertifikat, das die BlackBerry UEM-Verwaltungskonsole und BlackBerry UEM Self-Service zum Authentifizieren von Browsern verwenden. Wenn Sie eine hohe Verfügbarkeit konfigurieren, muss das Zertifikat den Namen der BlackBerry UEM-Domäne haben. Sie finden den BlackBerry UEM-Domänennamen in der Verwaltungskonsole unter Einstellungen > Infrastruktur > Instanzen.
SSL-Zertifikate für BlackBerry Web Services	Ein SSL-Zertifikat, das die BlackBerry Web Services zur Authentifizierung von Anwendungen verwendet, die die BlackBerry Web Services-APIs nutzen, um BlackBerry UEM zu verwalten. Wenn Sie eine hohe Verfügbarkeit konfigurieren, muss das Zertifikat den Namen der BlackBerry UEM-Domäne haben. Sie finden den BlackBerry UEM-Domänennamen in der Verwaltungskonsole unter Einstellungen > Infrastruktur > Instanzen.
Apple-Profil-Signaturzertifikat	Ein Zertifikat, das BlackBerry UEM zur Signierung des MDM-Profils verwendet, das Benutzer akzeptieren müssen, wenn sie iOS-Geräte aktivieren. Wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde, stellen Sie sicher, dass das Stammzertifikat für die Zertifizierungsstelle vor der Aktivierung auf den iOS-Geräten der Benutzer installiert wurde.
SSL-Zertifikat für BlackBerry Dynamics-Apps	Ein SSL-Zertifikat, das BlackBerry Dynamics Launcher zum Herstellen eines sicheren Kommunikationskanals mit BlackBerry UEM verwendet. BlackBerry Dynamics-Apps, die die integrierte BlackBerry Dynamics Launcher enthalten, können BlackBerry UEM das Zertifikat für die Authentifizierung beim Server präsentieren.
Zertifikat für BlackBerry Dynamics-Server	Ein SSL-Zertifikat, das Verbindungen zwischen BlackBerry UEM und BlackBerry Proxy authentifiziert.

Zertifikat	Beschreibung
Zertifikat für Anwendungsverwaltung	Ein SSL-Zertifikat, das für die Authentifizierung zwischen BlackBerry UEM- und BlackBerry Dynamics-Apps verwendet wird. Das Stammzertifizierungsstellenzertifikat für dieses Zertifikat wird in der Liste der vertrauenswürdigen CA-Zertifikate auf dem Gerät gespeichert. Wenn der Server sich bei dem Gerät authentifiziert, präsentiert der Server dem Gerät dieses Zertifikat für die Validierung. Wenn Sie dieses Zertifikat ändern und die Änderung wirksam wird, bevor BlackBerry UEM das Zertifikat an alle BlackBerry Dynamics-Apps sendet, müssen alle Apps, die das Zertifikat nicht erhalten haben, erneut aktiviert werden.
Zertifikat für Direct Connect	Ein SSL-Zertifikat, das für die Authentifizierung zwischen Direct Connect und BlackBerry Dynamics und anderen Komponenten verwendet wird. Wenn Sie dieses Zertifikat ändern und die Änderung wirksam wird, bevor BlackBerry UEM das Zertifikat an alle BlackBerry Dynamics-Apps sendet, müssen alle Apps, die das Zertifikat nicht erhalten haben, erneut aktiviert werden. Weitere Informationen zum Einrichten von Direct Connect finden Sie unter Konfigurieren von Direct Connect mit BlackBerry UEM

Überlegungen zum Ändern von BlackBerry Dynamics-Zertifikaten

Wenn Sie BlackBerry Dynamics-SSL-Zertifikate ändern möchten, berücksichtigen Sie die folgenden Überlegungen. Wenn Probleme auftreten, wenn Sie ein Zertifikat ändern, kann die Kommunikation zwischen den BlackBerry UEM-Komponenten und zwischen BlackBerry UEM und BlackBerry Dynamics-Apps gestört werden. Planen und testen Sie Zertifikatänderungen sorgfältig.

Neue Zertifikate zu peripheren Geräten hinzufügen

Wenn Sie BlackBerry Dynamics-Zertifikate zu peripheren Geräten auf Ihrem Netzwerk hinzugefügt haben, fügen Sie das neue Zertifikat zu den peripheren Geräten hinzu, bevor Sie es zur BlackBerry UEM hinzufügen.

BlackBerry Dynamics-Apps aktualisieren

Wenn Sie das BlackBerry Dynamics-Zertifikat für Anwendungsverwaltung oder Direct Connect ersetzen, stellen Sie sicher, dass die BlackBerry Dynamics-Apps der Benutzer auf die aktuellsten Versionen aktualisiert werden, bevor Sie das Zertifikat ersetzen.

Alle BlackBerry Dynamics-Apps, die von Ihrem Unternehmen entwickelt wurden, müssen mit Version 3.2 oder höher von BlackBerry Dynamics SDK erstellt werden. Ältere Apps können das neue Zertifikat von BlackBerry UEM nicht empfangen.

BlackBerry Dynamics-Apps müssen geöffnet sein, um ein Zertifikat zu empfangen.

Benutzer müssen eine BlackBerry Dynamics-App öffnen, damit die App ein Zertifikat von BlackBerry UEM empfängt. Wenn Sie das BlackBerry Dynamics-Zertifikat für Anwendungsverwaltung oder Direct Connect ändern und die Änderung wirksam wird, bevor BlackBerry UEM das Zertifikat an alle BlackBerry Dynamics-Apps sendet, müssen alle Apps, die das Zertifikat nicht erhalten haben, erneut aktiviert werden. Apps empfangen keine

Zertifikate, während sie auf iOS-Geräten ausgeschlossen sind oder während sich Android-Geräte im Ruhemodus befinden.

Sicherstellen, dass BlackBerry Connectivity Node erreichbar ist

Wenn BlackBerry Proxy-Instanzen von BlackBerry UEM nicht erreichbar sind, wenn BlackBerry Dynamics-Zertifikate ersetzt werden, können BlackBerry Dynamics-Apps nach dem Zertifikatersatz keine Verbindung zu diesen Instanzen herstellen.

Zertifikatänderungen angemessen planen

Wenn Sie das Zertifikat für BlackBerry Dynamics-Server ersetzen, wählen Sie einen Zeitraum mit niedriger Aktivität, um die Server neu zu starten.

Planen Sie ausreichend Zeit ein, damit die neuen Zertifikate auf die BlackBerry Proxy- und BlackBerry Dynamics-Apps propagiert werden können. Wenn Sie nur das Zertifikat für BlackBerry Dynamics-Server ersetzen, sollten Sie mindestens 10 Minuten vergehen lassen, bevor Sie den Server neu starten.

Wenn Sie das BlackBerry Dynamics-Zertifikat für Anwendungsverwaltung oder Direct Connect ersetzen, empfiehlt es sich, dass die Zeit bis zum Stichtag länger ist als die Einstellung „Letzte Kontaktzeit“ unter „Verbindung überprüfen“ im Konformitätsprofil.

Wenn Sie sowohl die BlackBerry Dynamics-Zertifikate für Anwendungsverwaltung und Direct Connect ersetzen, legen Sie die Gültigkeitszeiten mit einem Abstand von mindestens 30 Minuten fest. Wenn Sie eine große Anzahl von Benutzern und BlackBerry Dynamics-Apps haben, warten Sie länger als 30 Minuten zwischen jedem Zertifikat.

Ändern eines BlackBerry UEM-Zertifikats

Bevor Sie beginnen:

- Rufen Sie ein Zertifikat ab, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde. Das Zertifikat muss ein Schlüsselspeicher-Format (.pfx, .pkcs12) aufweisen.
- Wenn Sie das BlackBerry Dynamics-Zertifikat für Anwendungsverwaltung oder Direct Connect ersetzen, stellen Sie sicher, dass die BlackBerry Dynamics-Apps der Benutzer zunächst auf die aktuellsten Versionen aktualisiert werden.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Infrastruktur > Serverzertifikate**.
2. Klicken Sie im Abschnitt für das Zertifikat, das Sie ersetzen möchten, auf **Details anzeigen**.
3. Klicken Sie auf **Zertifikat ersetzen**.
4. Navigieren Sie zur Zertifikatsdatei, und wählen Sie sie aus.
5. Geben Sie ein Verschlüsselungskennwort für das Zertifikat ein.
6. Wenn Sie das Zertifikat für BlackBerry Dynamics-Server ersetzen, legen Sie fest, wann BlackBerry UEM neustarten soll, um die Änderung zu übernehmen.

   Es wird empfohlen, dass Sie einen Zeitraum mit geringer Aktivität für den Neustart der Server wählen.
7. Wenn Sie das BlackBerry Dynamics-Zertifikat für Anwendungsverwaltung oder Direct Connect ersetzen, geben Sie das Gültigkeitsdatum für die Zertifikatänderung an.

   Es wird empfohlen, dass das Gültigkeitsdatum nach dem bei „Letzte Kontaktzeit“ unter „Verbindung überprüfen“ im Konformitätsprofil festgelegten Datum liegt. Wenn Sie mehr als ein Zertifikat ändern, müssen die Gültigkeitszeiten mindestens 30 Minuten auseinander liegen.
8. Klicken Sie auf **Ersetzen**.

Wenn Sie fertig sind:

- Wenn Sie eines der Zertifikate auf der Registerkarte **Serverzertifikate** ersetzt haben, starten Sie den BlackBerry UEM Core-Service auf allen Servern neu. Es wird empfohlen, dass Sie einen Zeitraum mit geringer Aktivität für den Neustart der Server wählen.
- Für Zertifikate auf der Registerkarte BlackBerry Dynamics-Zertifikate können Sie auf **Auf Standard zurücksetzen** klicken, um zur Verwendung eines selbst signierten Zertifikats zurück zu wechseln.
- Auf der Registerkarte BlackBerry Dynamics-Zertifikate können Sie die Kontrollkästchen **BlackBerry UEM-Zertifizierungsstelle vertrauen** und **BlackBerry Dynamics-Zertifizierungsstelle vertrauen** deaktivieren, wenn es nicht mehr erforderlich ist, den selbst-signierten Zertifikaten zu vertrauen. Sie können das Kontrollkästchen **BlackBerry Dynamics-Zertifizierungsstelle vertrauen** nur deaktivieren, wenn Sie alle Zertifikate auf der Registerkarte BlackBerry Dynamics-Zertifikate ersetzt haben.
- Wenn BlackBerry Dynamics-Apps nach dem Ändern der Zertifikate nicht mehr kommunizieren, stellen Sie sicher, dass die Apps auf dem neuesten Stand sind, und weisen Sie dann die Benutzer an, die Apps erneut zu aktivieren.

Konfigurieren von BlackBerry UEM zum Senden von Daten über einen Proxy-Server

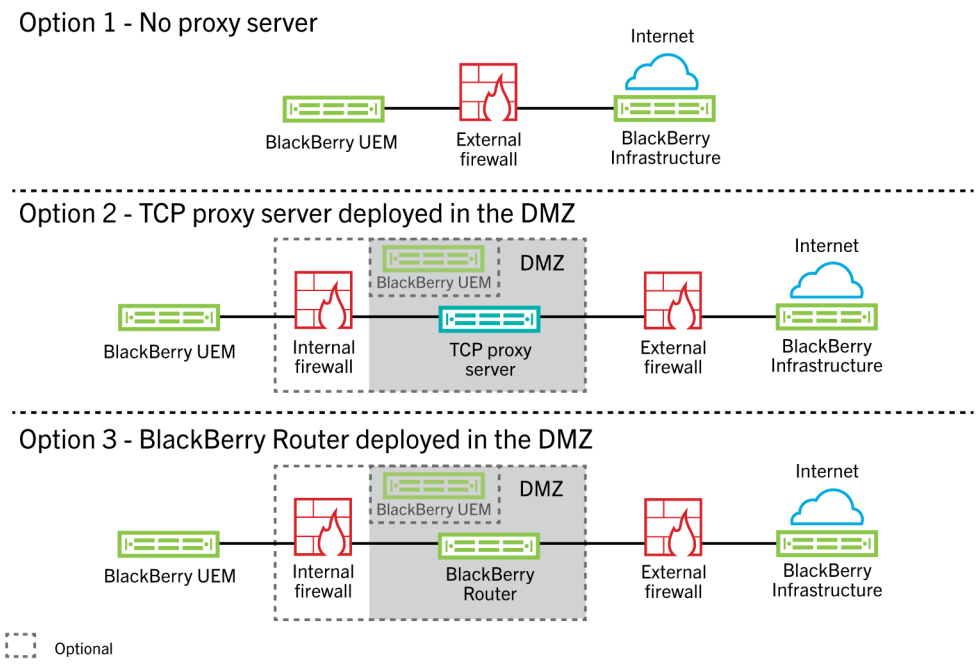
Sie können BlackBerry UEM so konfigurieren, dass Daten zuerst über einen TCP-Proxyserver oder eine Instanz des BlackBerry Router gesendet werden, bevor sie die BlackBerry Infrastructure erreichen.

Standardmäßig stellt BlackBerry UEM über Port 3101 eine direkte Verbindung mit der BlackBerry Infrastructure her. Wenn die Sicherheitsrichtlinie Ihres Unternehmens jedoch vorschreibt, dass interne Systeme keine direkten Verbindungen mit dem Internet herstellen dürfen, können Sie den BlackBerry Router oder einen TCP-Proxyserver installieren. Der BlackBerry Router bzw. der TCP-Proxy-Server fungiert als Vermittler zwischen BlackBerry UEM und der BlackBerry Infrastructure.

Sie können einen BlackBerry Router oder einen Proxyserver außerhalb der Unternehmens-Firewall in einer DMZ installieren. Durch die Installation des BlackBerry Router oder eines TCP-Proxy-Servers in einer DMZ wird die Sicherheit für BlackBerry UEM zusätzlich erhöht. Nur der BlackBerry Router oder der Proxy-Server stellen von außerhalb der Firewall eine Verbindung zu BlackBerry UEM her. Alle Verbindungen zur BlackBerry Infrastructure zwischen BlackBerry UEM und den Geräten werden über den BlackBerry Router oder den Proxy-Server geleitet.

Bei BlackBerry OS-Geräten (Version 5.0 bis 7.1) sendet der BlackBerry Router Daten auch direkt an Geräte und empfängt Daten von Geräten, die mit einem geschäftlichen Wi-Fi-Netzwerk oder mit einem Computer mit BlackBerry Device Manager verbunden sind.

Diese Abbildung zeigt die folgenden Optionen, die zum Senden von Daten über einen Proxyserver an die BlackBerry Infrastructure genutzt werden können: kein Proxyserver, TCP-Proxyserver in einer DMZ und BlackBerry Router in einer DMZ.



Senden von Daten über einen TCP-Proxyserver an die BlackBerry Infrastructure

Sie können einen transparenten TCP-Proxy-Server für den BlackBerry UEM Core-Dienst und einen weiteren transparenten TCP-Proxy-Server für den BlackBerry Affinity Manager-Dienst konfigurieren. Diese Dienste erfordern eine ausgehende Verbindung, für die möglicherweise auch unterschiedliche Ports konfiguriert werden müssen. Sie können nicht mehrere transparente TCP-Proxy-Server für den jeweiligen Dienst installieren oder konfigurieren.

Sie können jedoch mehrere TCP-Proxy-Server, die mit SOCKS v5 (keine Authentifizierung) konfiguriert wurden, für die Verbindung mit BlackBerry UEM festlegen. Mehrere TCP-Proxy-Server mit SOCKS v5-Konfiguration (keine Authentifizierung) können Unterstützung bereitstellen, wenn eine der aktiven Proxy-Serverinstanzen nicht ordnungsgemäß funktioniert.

Sie konfigurieren nur einen einzelnen Port, der von allen Dienstinstanzen mit SOCKS v5 überwacht wird. Wenn Sie mehr als einen TCP-Proxyserver mit SOCKS v5 konfigurieren, muss der Überwachungsport für jeden freigegeben werden.

Vergleichen von TCP-Proxys

Proxy	Beschreibung
Transparenter TCP-Proxy	• Fängt die normale Kommunikation auf Netzwerkebene ohne spezielle Client-Konfiguration ab • Keine Client-Browser-Konfiguration erforderlich • Befindet sich in der Regel zwischen Client und Internet • Führt Funktionen eines Gateways oder Routers aus • Wird häufig zur Durchsetzung von Richtlinien für die zulässige Nutzung verwendet • Wird von Internetdienstanbietern in einigen Ländern häufig verwendet, um Upstream-Bandbreite einzusparen und Kundenreaktionszeiten durch Zwischenspeicherung zu verbessern
SOCKS v5-Proxy	• Ein Internetprotokoll für die Verarbeitung von Internetdatenverkehr über einen Proxy-Server • Die Verarbeitung ist mit nahezu jeder TCP/UDP-Anwendung möglich, einschließlich Browsern und FTP-Clients, die SOCKS unterstützen • Kann eine gute Lösung für Internetanonymität und -sicherheit sein • Leitet Netzwerkpakete zwischen einem Client und einem Server über einen Proxy-Server weiter • Bietet Authentifizierungsmöglichkeiten, sodass nur autorisierte Benutzer auf einen Server zugreifen können • Leitet TCP-Verbindungen an eine beliebige IP-Adresse weiter • Ermöglicht die Anonymisierung von UDP- und TCP-Protokollen wie HTTP

Konfigurieren von BlackBerry UEM für die Verwendung eines transparenten TCP-Proxy-Servers

Bevor Sie beginnen: Installieren Sie einen kompatiblen transparenten TCP-Proxy-Server in der BlackBerry UEM-Domäne.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Infrastruktur > BlackBerry-Router und -Proxy**.

2. Wählen Sie die Option **Proxy-Server**.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Weiterleiten von TCP-Daten über einen TCP-Proxy-Server.	Geben Sie in den Feldern **BlackBerry UEM Core, BlackBerry Secure Gateway Service** den FQDN oder die IP-Adresse und die Portnummer des Proxyservers ein. In jedes Feld muss ein einzelner Wert eingegeben werden.
Weiterleiten von SRP-Datenverkehr über einen TCP-Proxy-Server.	Geben Sie in den Feldern für **Affinity Manager** den FQDN oder die IP-Adresse und die Portnummer des Proxy-Servers ein. In jedes Feld muss ein einzelner Wert eingegeben werden.
Weiterleiten von BlackBerry Secure Connect Plus-Datenverkehr über einen TCP-Proxy-Server.	Geben Sie in den Feldern **BlackBerry Secure Connect Plus** den FQDN oder die IP-Adresse und die Portnummer des Proxy-Servers ein. In jedes Feld muss ein einzelner Wert eingegeben werden.

4. Klicken Sie auf **Speichern**.

Aktivieren von SOCKS v5 auf einem TCP-Proxy-Server

Bevor Sie beginnen: Installieren Sie einen kompatiblen TCP-Proxy-Server mit SOCKS v5 (ohne Authentifizierung) in der BlackBerry UEM-Domäne.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Infrastruktur > BlackBerry-Router und -Proxy**
2. Wählen Sie die Option **Proxy-Server**.
3. Aktivieren Sie das Kontrollkästchen **SOCKS v5 aktivieren**.
4. Klicken Sie auf +.
5. Geben Sie in das Feld **Serveradresse** die IP-Adresse oder den Hostnamen des SOCKS v5-Proxy-Servers ein.
6. Klicken Sie auf **Hinzufügen**.
7. Wiederholen Sie die Schritte 1 bis 6 für jeden zu konfigurierenden SOCKS v5-Proxy-Server.
8. Geben Sie im Feld **Port** die Portnummer ein.
9. Klicken Sie auf **Speichern**.

Senden von Daten über den BlackBerry Router an die BlackBerry Infrastructure

Sie können mehrere Instanzen des BlackBerry Router für hohe Verfügbarkeit konfigurieren. Sie konfigurieren nur einen Port für die Überwachung durch BlackBerry Router-Instanzen.

BlackBerry UEM bietet keine Unterstützung für eine BlackBerry Router-Instanz, die ursprünglich mit BES5 verwendet wurde.

Standardmäßig stellt BlackBerry UEM eine Verbindung zum BlackBerry Router über Port 3102 für BlackBerry UEM-Dienste und Port 3101 für BES5-Dienste her. Der BlackBerry Router unterstützt den gesamten ausgehenden Datenverkehr von BlackBerry UEM Core und BlackBerry Affinity Manager.

Hinweis: Wenn ein anderer Port als der Standardport für den BlackBerry Router verwendet werden soll, finden Sie weitere Informationen unter support.blackberry.com/community im Artikel 36385.

Konfigurieren von BlackBerry UEM für die Verwendung von BlackBerry Router

Bevor Sie beginnen: Installieren Sie den BlackBerry Router in der BlackBerry UEM-Domäne. Anweisungen zum Installieren des BlackBerry Router finden Sie in der Dokumentation zu Installation und Upgrade.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Infrastruktur > BlackBerry-Router und -Proxy**.
2. Wählen Sie die Option **BlackBerry Router**.
3. Klicken Sie auf +.
4. Geben Sie die IP-Adresse oder den Hostnamen der BlackBerry Router-Instanz ein, zu der BlackBerry UEM eine Verbindung herstellen soll.
5. Klicken Sie auf **Hinzufügen**.
6. Wiederholen Sie die Schritte 1 bis 5 für jede BlackBerry Router-Instanz, die Sie konfigurieren möchten.
7. Geben Sie in das Feld **Port** die Portnummer ein, die von allen BlackBerry Router-Instanzen überwacht wird. Der Standardwert ist 3102.
8. Klicken Sie auf **Speichern**.

Senden von Daten über einen HTTP-Proxy an BlackBerry Dynamics NOC

Sie können BlackBerry UEM so konfigurieren, dass Daten über einen HTTP-Proxy zwischen BlackBerry UEM und BlackBerry Dynamics NOC gesendet werden.

Hinweis: Der Proxy muss über Port 443 auf BlackBerry Dynamics NOC zugreifen können. Weitere Informationen zu den Portanforderungen finden Sie unter Ausgehende Verbindungen:BlackBerry UEM zu BlackBerry Dynamics NOC.

Konfigurieren der HTTP-Proxy-Einstellungen

1. Klicken Sie in der Menüleiste auf **Einstellungen > Infrastruktur > BlackBerry-Router und -Proxy**.
2. Wählen Sie **HTTP-Proxy aktivieren** aus.
3. Wählen Sie eine der folgenden Optionen aus:
   - **Über Proxy nur mit NOC-Servern von BlackBerry Dynamics verbinden**
   - **Über Proxy mit allen Servern verbinden**
   - **Über Proxy nur mit bestimmten Servern verbinden**
4. Wenn Sie den Proxy verwenden möchten, um eine Verbindung mit den angegebenen Servern herzustellen, klicken Sie auf +, um zusätzliche Server anzugeben.
5. Geben Sie in das Feld **Adresse** die Adresse für den Proxyserver ein
6. Geben Sie im Feld **Port** die vom Proxy-Server überwachte Portnummer ein.
7. Wenn der Proxy-Server eine Authentifizierung benötigt, wählen Sie **Authentifizierung verwenden** und legen Sie den **Benutzernamen**, das **Kennwort** und, wenn nötig, die **Domäne** fest, die BlackBerry UEM für die Authentifizierung verwenden soll.
8. Klicken Sie auf **Speichern**.

Konfigurieren von Verbindungen über interne Proxy-Server

Wenn Ihr Unternehmen einen Proxyserver für Verbindungen zwischen den Servern in Ihrem Netzwerk nutzt, müssen Sie die serverseitigen Proxyeinstellungen möglicherweise so konfigurieren, dass BlackBerry UEM Core mit der BlackBerry UEM-Verwaltungskonsole kommunizieren kann, falls diese auf einem separaten Computer installiert wurde. Sie müssen möglicherweise auch die serverseitigen Proxy-Einstellungen konfigurieren, damit BlackBerry UEM mit anderen internen Diensten kommunizieren kann, wie z. B. Zertifizierungsstellen und Server, die Push-Anwendungen zur Übertragung von Daten an BlackBerry MDS Connection Service hosten.

Die serverseitigen Proxy-Einstellungen gelten nicht für ausgehende Verbindungen. Weitere Informationen zum Konfigurieren von BlackBerry UEM für die Verwendung eines TCP-Proxyservers finden Sie unter Konfigurieren von BlackBerry UEM zum Senden von Daten über einen Proxy-Server.

Konfigurieren von serverseitigen Proxyeinstellungen

Bevor Sie beginnen: Vergewissern Sie sich, dass Ihnen die PAC-URL oder der Hostname und die Portnummer sowie etwaige weitere Einstellungen zur Verfügung stehen, die Sie benötigen, um eine Verbindung zum Proxy-Server herzustellen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Infrastruktur > Serverseitiger Proxy**.
2. Wenn die meisten oder alle Server, die Bestandteil Ihrer BlackBerry UEM-Installation sind, eine Verbindung zu einem Proxy-Server herstellen müssen, führen Sie die folgenden Schritte durch, um globale serverseitige Proxy-Einstellungen festzulegen:
   a) Wählen Sie unter **Globale serverseitige Proxy-Einstellungen** in der Liste **Typ** die Option **PAC-Konfiguration** oder **Manuelle Konfiguration** aus.
   b) Geben Sie die Einstellungen an, die der Proxy-Server benötigt, und klicken Sie auf **Speichern**.
3. Wenn einer oder mehrere Server Proxy-Einstellungen benötigen, die sich von den globalen Einstellungen unterscheiden, führen Sie die folgenden Schritte durch, um die Proxy-Einstellungen für den Server festzulegen:
   a) Wählen Sie unter dem Servernamen in der Liste **Typ** die Option **Keine**, **PAC-Konfiguration** oder **Manuelle Konfiguration** aus.
   b) Wenn Sie **PAC-Konfiguration** oder **Manuelle Konfiguration** ausgewählt haben, geben Sie die vom Proxy-Server benötigten Einstellungen an.
   c) Klicken Sie auf **Speichern**.

Herstellen einer Verbindung zu Unternehmensverzeichnissen

Sie können BlackBerry UEM mit Ihrem Unternehmensverzeichnis verbinden, sodass der Zugriff auf die Benutzerliste Ihres Unternehmens möglich ist. Sie können BlackBerry UEM mit mehreren Verzeichnissen verbinden, und die Verzeichnisse können sich aus Microsoft Active Directory und LDAP zusammensetzen.

Wenn Ihr Unternehmensverzeichnis verbunden ist, können Sie die folgenden Funktionen nutzen:

- Sie können in BlackBerry UEM mit Benutzerdaten aus dem Verzeichnis Benutzerkonten erstellen, und BlackBerry UEM kann Administratoren für die Verwaltungskonsole und Benutzer für BlackBerry UEM Self-Service authentifizieren.
- Sie können Gruppen aus dem Unternehmensverzeichnis mit BlackBerry UEM-Gruppen verknüpfen, um Benutzer in BlackBerry UEM auf dieselbe Weise wie in Ihrem Unternehmensverzeichnis zu ordnen. Siehe Aktivieren von per Verzeichnis verknüpften Gruppen.
- Sie haben die Möglichkeit, für bestimmte Gruppen in Ihrem Unternehmensverzeichnis, Onboarding zu aktivieren, um BlackBerry UEM-Benutzer automatisch erstellen zu lassen. Wenn Sie Onboarding aktivieren, können Sie mithilfe von Offboarding-Konfigurationen auch Gerätedaten oder Benutzerkonten löschen, wenn Benutzer aus Gruppen in Ihrem Unternehmensverzeichnis entfernt werden. Siehe Aktivieren von Onboarding.

Wenn Sie BlackBerry UEM nicht mit einem Unternehmensverzeichnis verbinden, ist es möglich, lokale Benutzerkonten manuell zu erstellen und Administratoren über die Standardauthentifizierung anzumelden.

Führen Sie die folgenden Schritte aus, um BlackBerry UEM mit einem Unternehmensverzeichnis zu verbinden:

Schritt	Aktion
1	Stellen Sie eine Verbindung mit einer Microsoft Active Directory-Instanz oder einem LDAP-Verzeichnis her. Wenn in Ihrer Umgebung eine Ressourcengesamtstruktur enthalten ist, lesen Sie Konfigurieren der Microsoft Active Directory-Authentifizierung in einer Umgebung, die eine Ressourcengesamtstruktur enthält.
2	Aktivieren Sie optional per Verzeichnis verknüpfte Gruppen.
3	Aktivieren Sie optional Onboarding.
4	Fügen Sie optional einen Synchronisierungszeitplan hinzu.

Konfigurieren der Microsoft Active Directory-Authentifizierung in einer Umgebung, die eine Ressourcengesamtstruktur enthält

Wenn Ihre Unternehmensumgebung eine Ressourcengesamtstruktur enthält, die für das Ausführen von Microsoft Exchange verwendet wird, können Sie die Microsoft Active Directory-Authentifizierung für Benutzerkonten konfigurieren, die sich in vertrauenswürdigen Kontengesamtstrukturen befinden.

Wenn Ihre Umgebung eine Ressourcengesamtstruktur enthält, müssen Sie BlackBerry UEM in dieser installieren. In der Ressourcengesamtstruktur erstellen Sie für jedes Benutzerkonto ein Postfach und weisen die Postfächer den Benutzerkonten zu. Wenn Sie die Postfächer in der Ressourcengesamtstruktur Benutzerkonten in den Kontengesamtstrukturen zuweisen, erhalten die Benutzerkonten vollen Zugriff auf die Postfächer, und es wird eine Verbindung zwischen den Benutzerkonten in den Kontengesamtstrukturen und dem Microsoft Exchange-Server hergestellt.

Um Benutzer zu authentifizieren, die sich bei BlackBerry UEM anmelden, muss BlackBerry UEM die Benutzerinformationen lesen, die auf den zur Ressourcengesamtstruktur gehörenden globalen Katalogservern gespeichert sind. Sie müssen ein Microsoft Active Directory-Konto für BlackBerry UEM erstellen, das sich in einer Windows-Domäne befindet, die Teil der Ressourcengesamtstruktur ist. Beim Erstellen der Verzeichnisverbindung geben Sie die Windows-Domäne, den Benutzernamen und das Kennwort für das Microsoft Active Directory-Konto und ggf. die Namen der globalen Katalogserver an, die BlackBerry UEM nutzen kann.

Weitere Informationen finden Sie auf technet.microsoft.com unter *Verwalten verknüpfter Postfächer*.

Verbindung zu einer Microsoft Active Directory-Instanz

Bevor Sie beginnen: Erstellen Sie ein Microsoft Active Directory-Konto, das von BlackBerry UEM verwendet werden kann. Das Konto muss die folgenden Anforderungen erfüllen:

- Es muss sich in einer Windows-Domäne befinden, die Teil der Microsoft Exchange-Gesamtstruktur ist.
- Es muss Berechtigungen für den Zugriff auf den Benutzercontainer und Leseberechtigungen für die Benutzerobjekte aufweisen, die in den globalen Katalogservern in der Microsoft Exchange-Gesamtstruktur gespeichert sind.
- Das Kennwort muss so konfiguriert werden, dass es nicht abläuft und dass es bei der nächsten Anmeldung nicht geändert werden muss.
- Wenn Sie die einmalige Anmeldung aktivieren, muss die eingeschränkte Delegierung für das Konto konfiguriert werden.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf **Hinzufügen einer Microsoft Active Directory-Verbindung**.
3. Geben Sie im Feld **Name der Verbindung des Verzeichnisses** den Namen der Verzeichnisverbindung ein.
4. Geben Sie im Feld **Benutzername** den Benutzernamen für das Microsoft Active Directory-Konto ein.
5. Geben Sie im Feld **Domäne** den Namen der Windows-Domäne, die Teil der Microsoft Exchange-Gesamtstruktur ist, im DNS-Format ein (Beispiel: beispiel.com).
6. Geben Sie im Feld **Kennwort** das Kontokennwort ein.
7. Führen Sie in der Dropdown-Liste für die Auswahl der **Kerberos-Schlüsselverteilungscenter** eine der folgenden Aktionen durch:
   - Damit BlackBerry UEM die Schlüsselverteilungscenter (KDCs) automatisch erkennen kann, klicken Sie auf **Automatisch**.
   - Um die Liste der KDCs anzugeben, die BlackBerry UEM für die Authentifizierung verwenden soll, klicken Sie auf **Manuell**. Geben Sie im Feld **Servernamen** den Namen des KDC-Domänencontrollers im DNS-Format (z. B. kdc01.beispiel.com) ein. Fügen Sie optional die Portnummer ein, die der Domänencontroller verwendet (z. B. kdc01.beispiel.com:88). Klicken Sie auf + um zusätzliche KDC-Domänencontroller anzugeben, die BlackBerry UEM verwenden soll.
8. Führen Sie in der Dropdown-Liste **Auswahl des globalen Katalogs** eine der folgenden Aktionen aus:
   - Wenn BlackBerry UEM die globalen Katalogserver automatisch erkennen soll, klicken Sie auf **Automatisch**.
   - Um die Liste der globalen Katalogserver anzugeben, die BlackBerry UEM verwenden soll, klicken Sie auf **Manuell**. Geben Sie im Feld **Servernamen** den DNS-Namen des globalen Katalogservers ein, auf den

BlackBerry UEM zugreifen soll (z. B. globalcatalog01.beispiel.com). Fügen Sie optional die Portnummer ein, die der globale Katalogserver verwendet (z. B. globalcatalog01.com:3268). Klicken Sie auf +, um zusätzliche Server anzugeben.

9. Klicken Sie auf **Fortfahren**.
10. Führen Sie im Feld **Suchbasis des globalen Katalogs** eine der folgenden Aktionen aus:
    - Lassen Sie das Feld leer, um BlackBerry UEM zu ermöglichen, den globalen Katalog zu durchsuchen.
    - Geben Sie den Distinguished Name des Benutzercontainers ein (z. B. OU=sales,DC=example,DC=com), um zu steuern, welche Benutzerkonten BlackBerry UEM authentifizieren kann.
11. Wenn Sie die Unterstützung für globale Gruppen aktivieren möchten, klicken Sie in der Dropdown-Liste **Unterstützung für globale Gruppen** auf **Ja**.

    Wenn Sie für das Onboarding globale Gruppen verwenden möchten, müssen Sie **Ja** auswählen. Um eine globale Gruppendomäne zu konfigurieren, klicken Sie im Abschnitt **Liste der globalen Gruppendomänen** auf +. Wählen Sie im Feld **Domäne** die Domäne aus, die hinzugefügt werden soll. Die Standardauswahl für das Feld **Benutzername und Kennwort angeben?** ist „Nein“. Wenn Sie diese Standardauswahl beibehalten, werden der Benutzername und das Kennwort für die Verbindung mit der Gesamtstruktur verwendet. Wenn Sie „Ja“ wählen, müssen Sie gültige Anmeldeinformationen für ein Microsoft Active Directory-Konto in der ausgewählten Domäne angeben. Im Feld **KDC-Auswahl** können Sie „Automatisch“ auswählen, damit BlackBerry UEM Key Distribution Centers automatisch sucht. Wenn Sie „Manuell“ auswählen, können Sie die für die Authentifizierung zu verwendende KDC-Liste für BlackBerry UEM selbst angeben. Klicken Sie auf **Hinzufügen**.
12. Wenn Sie die Unterstützung für verknüpfte Microsoft Exchange-Postfächer aktivieren möchten, klicken Sie in der Dropdown-Liste **Unterstützung für verknüpfte Microsoft Exchange-Postfächer** auf **Ja**.

    Um das Microsoft Active Directory-Konto für jede Gesamtstruktur zu konfigurieren, auf die BlackBerry UEM zugreifen soll, klicken Sie im Abschnitt **Auflisten von Kontengesamtstrukturen** auf +. Geben Sie den Namen der Benutzerdomäne (der Benutzer kann einer beliebigen Domäne in der Kontengesamtstruktur angehören) sowie den Benutzernamen und das Kennwort an. Geben Sie bei Bedarf die KDCs an, die BlackBerry UEM durchsuchen soll. Geben Sie bei Bedarf die globalen Katalogserver an, auf die BlackBerry UEM zugreifen soll. Klicken Sie auf **Hinzufügen**.
13. Zum Aktivieren der einmaligen Anmeldung wählen Sie das Kontrollkästchen **Windows Single Sign-on aktivieren** aus. Weitere Informationen zu Single Sign-on finden Sie unter Konfigurieren der einmaligen Anmeldung für BlackBerry UEM.
14. Um weitere Benutzerdetails aus Ihrem Unternehmensverzeichnis zu synchronisieren, aktivieren Sie das Kontrollkästchen **Zusätzliche Benutzerdetails synchronisieren**. Zu den zusätzlichen Details gehören der Name des Unternehmens und die geschäftliche Telefonnummer.
15. Klicken Sie auf **Speichern**.
16. Klicken Sie auf **Schließen**.

Wenn Sie fertig sind: Informationen zum Hinzufügen eines Synchronisierungsplans für Verzeichnisse finden Sie unter Hinzufügen eines Synchronisationsplans.

Herstellen der Verbindung zu einem LDAP-Verzeichnis

Bevor Sie beginnen:

- Erstellen Sie ein LDAP-Konto für BlackBerry UEM im entsprechenden LDAP-Verzeichnis. Das Konto muss die folgenden Anforderungen erfüllen:
  - Das Konto verfügt über Leseberechtigungen für alle Benutzer im Verzeichnis.
  - Das Kennwort des Kontos läuft nie ab, und der Benutzer muss das Kennwort bei der nächsten Anmeldung nicht ändern.

- Wenn die LDAP-Verbindung mit SSL verschlüsselt ist, vergewissern Sie sich, dass Sie das Serverzertifikat für die LDAP-Verbindung haben und dass der LDAP-Server TLS 1.2 unterstützt. Wenn SSL aktiviert ist, muss die LDAP-Verbindung zu BlackBerry UEM TLS 1.2 verwenden.
- Überprüfen Sie die von Ihrem Unternehmen verwendeten LDAP-Attributwerte (die nachstehenden Schritte enthalten Beispiele für typische Attributwerte). Sie müssen die LDAP-Attributwerte aus Schritt 11 und den weiteren Schritten angeben.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf **Hinzufügen einer LDAP-Verbindung**.
3. Geben Sie im Feld **Name der Verbindung des Verzeichnisses** einen Namen für die Verzeichnisverbindung ein.
4. Führen Sie in der Dropdown-Liste **LDAP-Servererkennung** eine der folgenden Aktionen aus:
   - Für eine automatische Erkennung des LDAP-Servers, klicken Sie auf **Automatisch**. Geben Sie im Feld **DNS-Domänenname** den Domänennamen des Servers ein, der das Unternehmensverzeichnis hostet.
   - Um die Liste der LDAP-Server festzulegen, klicken Sie auf **Server aus der Liste unten auswählen**. Geben Sie in das Feld **LDAP-Server** den Namen des LDAP-Servers ein. Um weitere LDAP-Server hinzuzufügen, klicken Sie auf +.
5. Führen Sie in der Dropdown-Liste **SSL aktivieren** eine der folgenden Aktionen aus:
   - Wenn die LDAP-Verbindung eine SSL-Verschlüsselung aufweist, klicken Sie auf **Ja**. Klicken Sie neben dem Feld **SSL-Zertifikat des LDAP-Servers** auf **Durchsuchen**, und wählen Sie das LDAP-Serverzertifikat aus.
   - Wenn die LDAP-Verbindung keine SSL-Verschlüsselung aufweist, klicken Sie auf **Nein**.
6. Geben Sie im Feld **LDAP-Port** die TCP-Portnummer für die Verbindung ein. Die Standardwerte sind 636 für „SSL aktiviert“ oder 389 für „SSL deaktiviert“.
7. Führen Sie in der Dropdown-Liste **Autorisierung erforderlich** eine der folgenden Aktionen aus:
   - Wenn für die Verbindung eine Autorisierung erforderlich ist, klicken Sie auf **Ja**. Geben Sie im Feld **Anmeldung** den DN des Benutzers ein, der für die Anmeldung bei LDAP autorisiert ist (z. B. an=admin,o=Org1). Geben Sie im Feld **Kennwort** das Kennwort ein.
   - Wenn für die Verbindung keine Autorisierung erforderlich ist, klicken Sie auf **Nein**.
8. Geben Sie im Feld **Benutzersuchbasis** den Wert ein, der als Basis-DN für Benutzerinformationssuchen verwendet werden soll.
9. Geben Sie im Feld **LDAP-Suchfilter für Benutzer** den LDAP-Suchfilter ein, der zum Auffinden von Benutzerobjekten auf Ihrem Unternehmensverzeichnisserver erforderlich ist. Geben Sie beispielsweise für ein IBM Domino Directory Folgendes ein: `(objectClass=Person)`.

   Hinweis: Wenn Sie deaktivierte Benutzerkonten aus den Suchergebnissen ausschließen möchten, geben Sie Folgendes ein: `(&(objectclass=user)(logindisabled=false))`.
10. Führen Sie in der Dropdown-Liste **LDAP-Suchbereich für Benutzer** eine der folgenden Aktionen aus:
    - Klicken Sie für die Suche nach Objekten, die dem Basisobjekt folgen, auf **Alle Ebenen**. Dies ist die Standardeinstellung.
    - Um nach Objekten zu suchen, die sich direkt eine Ebene unter dem Basis-DN befinden, klicken Sie auf **Eine Ebene**.
11. Geben Sie im Feld **Eindeutige Kennung** den Namen des Attributs ein, das den jeweiligen Benutzer im LDAP-Verzeichnis Ihres Unternehmens eindeutig identifiziert (muss eine Zeichenfolge sein, die unveränderbar und global eindeutig ist). Zum Beispiel `dominoUNID` in IBM Domino LDAP 7 und höher.
12. Geben Sie im Feld **Vorname** das Attribut für den Vornamen der einzelnen Benutzer ein (beispielsweise: `givenName`).
13. Geben Sie im Feld **Nachname** das Attribut für den Nachnamen der einzelnen Benutzer ein (beispielsweise: `sn`).
14. Geben Sie im Feld **Anmeldeattribut** das für die Authentifizierung zu verwendende Anmeldeattribut ein (beispielsweise `uid`).

15. Geben Sie im Feld **E-Mail-Adresse** das Attribut für die E-Mail-Adresse der einzelnen Benutzer ein (beispielsweise `mail`). Wenn Sie keinen Wert festlegen, wird ein Standardwert verwendet.
16. Geben Sie im Feld **Anzeigename** das Attribut für den Anzeigenamen der einzelnen Benutzer ein (beispielsweise `displayName`). Wenn Sie keinen Wert festlegen, wird ein Standardwert verwendet.
17. Geben Sie im Feld **Kontoname des E-Mail-Profils** das Attribut für den Kontonamen des E-Mail-Profils der einzelnen Benutzer ein (beispielsweise: `mail`).
18. Geben Sie im Feld **Benutzerprinzipalname** den Benutzerprinzipalnamen für SCEP ein (beispielsweise `mail`).
19. Um per Verzeichnis verknüpfte Gruppen für die Verzeichnisverbindung zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktivieren von per Verzeichnis verknüpften Gruppen**.

    Geben Sie die folgenden Informationen an:

    - Geben Sie im Feld **Suchbasis für Gruppen** den Wert ein, der als Basis-DN für Gruppeninformationssuchen verwendet werden soll.
    - Geben Sie im Feld **LDAP-Suchfilter für Gruppen** den LDAP-Suchfilter ein, der zum Auffinden von Gruppenobjekten in Ihrem Unternehmensverzeichnis erforderlich ist. Geben Sie beispielsweise für IBM Domino Directory Folgendes ein: `(objectClass=dominoGroup)`.
    - Geben Sie im Feld **Eindeutige Kennung der Gruppe** das Attribut für die eindeutige Kennung der einzelnen Gruppen ein. Dieses Attribut muss unveränderbar und global eindeutig sein (z. B. `cn`).
    - Geben Sie im Feld **Anzeigename der Gruppe** das Attribut für den Anzeigenamen der einzelnen Gruppen ein (z. B. `cn`).
    - Geben Sie im Feld **Gruppenmitgliedschaftsattribut** das Attribut für den Mitgliedschaftsbezeichner der einzelnen Gruppen ein. Dieses Attribut muss unveränderbar und global eindeutig sein (z. B. `member`).
    - Geben Sie im Feld **Gruppenname testen** einen vorhandenen Gruppennamen ein, um die festgelegten Gruppenattribute zu validieren.
20. Klicken Sie auf **Speichern**.
21. Klicken Sie auf **Schließen**.

Wenn Sie fertig sind: Informationen zum Hinzufügen eines Synchronisierungsplans für Verzeichnisse finden Sie unter Hinzufügen eines Synchronisationsplans.

Aktivieren von per Verzeichnis verknüpften Gruppen

Bevor Sie beginnen: Vergewissern Sie sich, dass keine Synchronisierung des Unternehmensverzeichnisses ausgeführt wird. Sie können die Änderungen, die Sie an einer Unternehmensverzeichnisverbindung vornehmen, erst nach Beendigung der Synchronisierung speichern.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf den Namen des zu bearbeitenden Unternehmensverzeichnisses.
3. Aktivieren Sie auf der Registerkarte **Synchronisierungseinstellungen** das Kontrollkästchen **Aktivieren von per Verzeichnis verknüpften Gruppen**.
4. Um die Synchronisierung von Unternehmensverzeichnisgruppen zu erzwingen, aktivieren Sie das Kontrollkästchen **Synchronisierung erzwingen**.

   Wenn diese Option aktiviert ist und eine Gruppe aus dem Unternehmensverzeichnis entfernt wird, werden die Verknüpfungen für diese Gruppe aus den per Verzeichnis verknüpften Gruppen und den Onboarding-Verzeichnisgruppen entfernt. Wenn alle Unternehmensverzeichnisgruppen, die einer per Verzeichnis verknüpften Gruppe zugeordnet sind, entfernt werden, wird die per Verzeichnis verknüpfte Gruppe in eine lokale Gruppe umgewandelt. Wenn diese nicht ausgewählt sind und keine Unternehmensverzeichnisgruppe gefunden werden kann, wird der Synchronisierungsvorgang abgebrochen.
5. Geben Sie im Feld **Synchronisierungsbeschränkung** die maximale Anzahl Änderungen ein, die pro Synchronisierungsprozess zulässig sein sollen.

Die Standardeinstellung ist 5. Falls die Anzahl der zu synchronisierenden Änderungen das Synchronisierungslimit übersteigt, können Sie die Ausführung der Synchronisierung verhindern. Änderungen werden berechnet, indem die folgenden Elemente addiert werden: die den Gruppen hinzuzufügenden Benutzer, die aus den Gruppen zu entfernenden Benutzer, die per Onboarding zu integrierenden Benutzer, die durch Offboarding zu entfernenden Benutzer.

6. Geben Sie im Feld **Maximale Verschachtelung von Verzeichnisgruppen** die Anzahl der Verschachtelungsebenen ein, die für Unternehmensverzeichnisgruppen synchronisiert werden sollen.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Erstellen Sie einer per Verzeichnis verknüpfte Gruppe. Weitere Informationen finden Sie in der Dokumentation für Administratoren.

Aktivieren von Onboarding

Onboarding bedeutet, dass Benutzerkonten auf Grundlage der Benutzermitgliedschaft in einer universellen oder globalen Unternehmensverzeichnisgruppe automatisch zu BlackBerry UEM hinzugefügt werden können. Die Benutzerkonten werden BlackBerry UEM während des Synchronisierungsvorgangs hinzugefügt.

Außerdem können Sie auswählen, ob die per Onboarding integrierten Benutzer automatisch eine E-Mail-Nachricht und Aktivierungskennwörter oder Zugriffsschlüssel für BlackBerry Dynamics-Apps erhalten sollen.

Offboarding

Wenn Sie Onboarding aktivieren, können Sie auch den Offboarding-Vorgang konfigurieren. Wenn ein Benutzer aus allen Unternehmensverzeichnisgruppen in den Onboarding-Verzeichnisgruppen entfernt wird, kann BlackBerry UEM das Offboarding des Benutzers auf eine der folgenden Arten automatisch durchführen:

- Löschen der geschäftlichen Daten oder aller Daten von den Geräten der Benutzer
- Löschen des Benutzerkontos aus BlackBerry UEM

Mithilfe des Offboarding-Schutzes können Sie das Löschen von Gerätedaten oder Benutzerkonten um einen Synchronisierungszyklus verzögern, damit unerwartete Löschvorgänge vermieden werden, die aufgrund der Verzeichnisreplikationslatenz auftreten können. Unabhängig vom Synchronisierungsintervall nimmt die Verzögerung, die durch den Offboarding-Schutz bereitgestellt wird, jedoch mindestens zwei Stunden in Anspruch.

Hinweis: Die Offboarding-Einstellungen gelten auch für bestehende Verzeichnisbenutzer in BlackBerry UEM. Es wird empfohlen, durch Klicken auf das Vorschausymbol einen Verzeichnissynchronisierungsbericht zu erzeugen und die Änderungen zu überprüfen.

Synchronisierung

Nachdem Sie Offboarding aktiviert haben, werden die Offboarding-Regeln während der nächsten Synchronisierung auf alle Benutzer angewendet, die Sie vor der Aktivierung von Offboarding in der Verwaltungskonsole manuell hinzugefügt haben und die keine Mitglieder von Gruppen sind, die per Verzeichnis verknüpft sind.

Nach der Aktivierung von Onboarding können Sie BlackBerry UEM Benutzer auch dann manuell hinzufügen, wenn sie sich bereits in einer Gruppe befinden, die per Verzeichnis verknüpft ist. Wenn Offboarding aktiviert ist, werden bei der nächsten Synchronisierung Offboarding-Regeln auf die Geräte der Benutzer angewendet, die Sie BlackBerry UEM manuell hinzufügen, falls es sich zum Zeitpunkt der Synchronisierung nicht um Mitglieder einer Onboarding-Synchronisierungsgruppe handelt.

Aktivieren und Konfigurieren von Onboarding und Offboarding

Sie können Benutzer, die zu universellen und globalen Gruppen gehören, automatisch integrieren. Onboarding wird für lokale Domänengruppen nicht unterstützt.

Bevor Sie beginnen:

- Vergewissern Sie sich, dass keine Synchronisierung des Unternehmensverzeichnisses ausgeführt wird. Sie können die Änderungen, die Sie an einer Unternehmensverzeichnisverbindung vornehmen, erst nach Beendigung der Synchronisierung speichern.
- Um Mitglieder globaler Gruppen zu integrieren, müssen Sie die Unterstützung für globale Gruppen in den Verbindungseinstellungen von Microsoft Active Directory aktivieren.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf den Namen des zu bearbeitenden Unternehmensverzeichnisses.
3. Aktivieren Sie auf der Registerkarte **Synchronisierungseinstellungen** das Kontrollkästchen **Aktivieren von per Verzeichnis verknüpften Gruppen**.
4. Aktivieren Sie das Kontrollkästchen **Onboarding aktivieren**.
5. Führen Sie die folgenden Schritte für jede Gruppe durch, die Sie mit einer Geräteaktivierungsoption für Onboarding konfigurieren möchten:
   a) Klicken Sie auf +.
   b) Geben Sie den Namen der Unternehmensverzeichnisgruppe ein. Klicken Sie auf 🔍.
   c) Wählen Sie die Gruppe aus. Klicken Sie auf **Hinzufügen**.
   d) Wählen Sie optional **Verschachtelte Gruppen verknüpfen** aus.
   e) Geben Sie im Abschnitt **Geräteaktivierung** an, ob integrierte Benutzer ein automatisch generiertes Aktivierungskennwort oder kein Aktivierungskennwort erhalten sollen. Wenn Sie die Option für das automatisch generierte Kennwort auswählen, konfigurieren Sie den Aktivierungszeitraum und wählen eine Vorlage für die Aktivierungs-E-Mail aus.
6. Um das Onboarding von Benutzern mit BlackBerry Dynamics auszuführen, aktivieren Sie das Kontrollkästchen **Nur Benutzer mit BlackBerry Dynamics-Apps integrieren**.
7. Führen Sie die folgenden Schritte für jede Gruppe durch, die Sie per Onboarding aufnehmen möchten und die nur eine Aktivierung für BlackBerry Dynamics-Apps erhalten sollen:
   a) Klicken Sie auf +.
   b) Geben Sie den Namen der Unternehmensverzeichnisgruppe ein. Klicken Sie auf 🔍.
   c) Wählen Sie die Gruppe aus. Klicken Sie auf **Hinzufügen**.
   d) Wählen Sie optional **Verschachtelte Gruppen verknüpfen** aus.
   e) Wählen Sie die Anzahl der Zugriffsschlüssel aus, die pro hinzugefügtem Benutzer erzeugt werden sollen, den Ablauf des Zugriffsschlüssels und E-Mail-Vorlage.
8. Wenn Gerätedaten beim Offboarding eines Benutzers gelöscht werden sollen, aktivieren Sie das Kontrollkästchen **Gerätedaten löschen, wenn der Benutzer von allen integrierten Verzeichnisgruppen entfernt wird**. Wählen Sie eine der folgenden Optionen aus:
   - Nur geschäftliche Daten löschen
   - Alle Gerätedaten löschen
   - Alle Gerätedaten für Eigentum des Unternehmens löschen/Nur Geschäftsdaten für Privateigentum löschen
9. Um ein Benutzerkonto aus BlackBerry UEM zu löschen, wenn ein Benutzer aus allen Onboarding-Gruppen entfernt wird, aktivieren Sie das Kontrollkästchen **Benutzer löschen, wenn der Benutzer von allen integrierten Verzeichnisgruppen entfernt wird**. Beim ersten Synchronisierungszyklus, der durchgeführt wird, nachdem ein Benutzerkonto aus allen Onboarding-Verzeichnisgruppen entfernt wurde, wird das Benutzerkonto aus BlackBerry UEM gelöscht.

10. Um zu verhindern, dass Benutzerkonten oder Gerätedaten unerwartet aus BlackBerry UEM gelöscht werden, wählen Sie **Offboarding-Schutz** aus.

    Offboarding-Schutz bedeutet, dass Benutzer nicht aus BlackBerry UEM gelöscht werden, es sei denn, ihr Benutzerkonto befindet sich in zwei aufeinanderfolgenden Synchronisierungszyklen nicht in den Onboarding-Verzeichnisgruppen. Unabhängig vom Synchronisierungsintervall nimmt die Verzögerung, die durch den Offboarding-Schutz bereitgestellt wird, jedoch mindestens zwei Stunden in Anspruch.
11. Um die Synchronisierung von Unternehmensverzeichnisgruppen zu erzwingen, aktivieren Sie das Kontrollkästchen **Synchronisierung erzwingen**.

    Wenn diese Option aktiviert ist und eine Gruppe aus dem Unternehmensverzeichnis entfernt wird, werden die Verknüpfungen für diese Gruppe aus den Onboarding-Verzeichnisgruppen und den per Verzeichnis verknüpften Gruppen entfernt. Wenn diese Option nicht aktiviert ist und eine Unternehmensverzeichnisgruppe gefunden werden kann, wird der Synchronisierungsvorgang abgebrochen.
12. Geben Sie im Feld **Synchronisierungsbeschränkung** die maximale Anzahl Änderungen ein, die pro Synchronisierungsprozess zulässig sein sollen. Die Standardeinstellung lautet fünf.

    Falls die Anzahl der zu synchronisierenden Änderungen das Synchronisierungslimit übersteigt, können Sie die Ausführung der Synchronisierung verhindern. Änderungen werden berechnet, indem die folgenden Elemente addiert werden: die den Gruppen hinzuzufügenden Benutzer, die aus den Gruppen zu entfernenden Benutzer, die per Onboarding zu integrierenden Benutzer, die durch Offboarding zu entfernenden Benutzer.
13. Geben Sie im Feld **Maximale Verschachtelung von Verzeichnisgruppen** die Anzahl der Verschachtelungsebenen ein, die für Unternehmensverzeichnisgruppen synchronisiert werden sollen.
14. Klicken Sie auf **Speichern**.

Synchronisieren einer Unternehmensverzeichnis-Verbindung

Bevor Sie beginnen: Vorschau des Synchronisationsberichts

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie in der Spalte **Synchronisierung** auf .

Wenn Sie fertig sind: Anzeigen eines Synchronisierungsberichts

Vorschau des Synchronisationsberichts

In der Vorschau eines Synchronisationsberichts können Sie vor der Synchronisierung überprüfen, ob geplante Updates Ihren Erwartungen entsprechen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie in der Spalte **Vorschau** auf .
3. Klicken Sie auf **Jetzt Vorschau anzeigen**.
4. Wenn die Verarbeitung des Berichts abgeschlossen ist, klicken Sie auf das Datum in der Spalte **Letzter Bericht**.
5. Klicken Sie zum Anzeigen der zuletzt erzeugten Synchronisierungsberichte auf das Dropdown-Menü.

Anzeigen eines Synchronisierungsberichts

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie in der Spalte **Letzter Bericht** auf das Datum.
3. Klicken Sie zum Anzeigen der zuletzt erzeugten Synchronisierungsberichte auf das Dropdown-Menü.

Hinzufügen eines Synchronisationsplans

Sie können einen Synchronisierungszeitplan hinzufügen, um BlackBerry UEM automatisch mit dem Firmenverzeichnis Ihres Unternehmens zu synchronisieren. Es gibt drei Arten von Synchronisierungszeitplänen:

- Intervall: Sie geben den Zeitraum zwischen den einzelnen Synchronisierungen, den Zeitrahmen und die Tage an, an denen die Synchronisierung erfolgt.
- Einmal täglich: Sie geben die Tageszeit an, zu der die Synchronisierung beginnt, und die Tage, an denen sie erfolgt.
- Keine Wiederholung: Sie geben die Uhrzeit und den Tag für eine einmalige Synchronisierung an.

Im Bildschirm „Unternehmensverzeichnis“ können Sie BlackBerry UEM jederzeit manuell mit Ihrem Unternehmensverzeichnis synchronisieren.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf den Namen des zu bearbeitenden Unternehmensverzeichnisses.
3. Klicken Sie auf der Registerkarte **Synchronisierungszeitplan** auf +.
4. Um die Menge der zu synchronisierenden Informationen zu reduzieren, wählen Sie in der Dropdown-Liste **Synchronisierungstyp** eine der folgenden Optionen aus:
   - **Alle Gruppen und Benutzer**: Dies ist die Standardeinstellung. Wenn Sie diese Option auswählen, erfolgt das Onboarding, Offboarding und die Verlinkung von Benutzern in per Verzeichnis verknüpften Gruppen während der Synchronisierung. Benutzer, die nicht integriert oder entfernt werden, aber die per Verzeichnis verknüpften Gruppen ändern, und Benutzer, deren Attribute geändert werden, werden synchronisiert.
   - **On-Boarding-Gruppen**: Wenn Sie diese Option auswählen, erfolgt das Onboarding, Offboarding und die Verlinkung von Benutzern in per Verzeichnis verknüpften Gruppen während der Synchronisierung. Benutzer, deren Attribute geändert werden, werden synchronisiert. Benutzer, die nicht integriert oder entfernt werden, aber die per Verzeichnis verknüpften Gruppen ändern, werden nicht synchronisiert.
   - **Per Verzeichnis verknüpfte Gruppen**: Wenn Sie diese Option auswählen, erfolgt das Onboarding und Offboarding von Benutzern nicht während der Synchronisierung. Benutzer, deren per Verzeichnis verknüpfte Gruppen geändert werden, werden entsprechend verknüpft. Benutzer, deren Attribute geändert werden, werden synchronisiert.
   - **Benutzerattribute**: Wenn Sie diese Option auswählen, erfolgt das Onboarding und Offboarding von Benutzern nicht während der Synchronisierung. Benutzer, deren per Verzeichnis verknüpfte Gruppen geändert werden, werden nicht synchronisiert. Benutzer, deren Attribute geändert werden, werden synchronisiert.
5. Wählen Sie in der Dropdown-Liste **Wiederholung** eine der folgenden Optionen aus:

Option	Schritte
Intervall	**a.** Geben Sie im Feld **Intervall** die Zeit zwischen den einzelnen Synchronisierungsvorgängen in Minuten ein. **b.** Geben Sie den Zeitrahmen für die Synchronisierung an. **c.** Wählen Sie die Wochentage aus, an denen die Synchronisierungen erfolgen sollen.
Einmal täglich	**a.** Geben Sie an, wann die Synchronisierung gestartet werden soll. **b.** Wählen Sie die Wochentage aus, an denen die Synchronisierungen erfolgen sollen.
Keine Wiederholung	**a.** Geben Sie an, wann die Synchronisierung gestartet werden soll. **b.** Wählen Sie den Tag aus, an dem die Synchronisierung stattfinden soll.

6. Klicken Sie auf **Hinzufügen**.

Herstellen einer Verbindung zu einem SMTP-Server zum Senden von E-Mail-Benachrichtigungen

Damit BlackBerry UEM E-Mail-Benachrichtigungen senden kann, muss eine Verbindung zwischen BlackBerry UEM und dem SMTP-Server bestehen.

BlackBerry UEM sendet über E-Mail-Benachrichtigungen Aktivierungsanweisungen an Benutzer. Sie können BlackBerry UEM auch so konfigurieren, dass Kennwörter für BlackBerry UEM Self-Service und Warnungen zu Vorschrifteneinhaltung auf Geräten oder E-Mail-Nachrichten an Einzelpersonen gesendet werden.

Wenn keine Verbindung zwischen BlackBerry UEM und SMTP-Server besteht, ist BlackBerry UEM nicht in der Lage, Kennwörter, Aktivierungs- oder E-Mail-Nachrichten zu senden. Sie können BlackBerry UEM jedoch trotzdem so konfigurieren, dass Warnmeldungen zur Vorschrifteneinhaltung direkt an Geräte gesendet werden.

Weitere Informationen zu Aktivierungsnachrichten, Warnmeldungen zur Vorschrifteneinhaltung auf Geräten und zum Senden einzelner E-Mail-Nachrichten finden Sie in der Dokumentation für Administratoren.

Herstellen einer Verbindung zu einem SMTP-Server zum Senden von E-Mail-Benachrichtigungen

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > SMTP-Server**.
2. Klicken Sie auf ✎.
3. Geben Sie in das Feld **Angezeigter Name des Absenders** einen Namen ein, der für BlackBerry UEM-E-Mail-Benachrichtigungen verwendet werden soll. Zum Beispiel `donotreply` oder `BUEM Admin`.
4. Geben Sie in das Feld **Absenderadresse** die E-Mail-Adresse ein, die BlackBerry UEM zum Senden von E-Mail-Benachrichtigungen verwenden soll.
5. Geben Sie in das Feld **SMTP-Server** den FQDN des SMTP-Servers ein. Beispiel: `mail.example.com`.
6. Geben Sie im Feld **SMTP-Serverport** die Portnummer des SMTP-Servers ein. Die Standardportnummer ist 25.
7. Wählen Sie im Dropdown-Menü **Unterstützte Verschlüsselungsmethode** die Verschlüsselung aus, die auf E-Mail-Nachrichten angewendet werden soll.
8. Wenn der SMTP-Server eine Authentifizierung erfordert, geben Sie im Feld **Benutzername** den Anmeldenamen des SMTP-Servers ein. Geben Sie im Feld **Kennwort** das Kennwort des SMTP-Servers ein.
9. Importieren Sie ggf. ein SMTP-Zertifizierungsstellenzertifikat:
   a) Kopieren Sie die SSL-Zertifikatsdatei für den SMTP-Server Ihres Unternehmens auf den von Ihnen verwendeten Computer.
   b) Klicken Sie auf **Durchsuchen**.
   c) Navigieren Sie zur SSL-Zertifikatsdatei, und klicken Sie auf **Hochladen**.
10. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Klicken Sie auf **Verbindung testen**, wenn Sie die Verbindung zum SMTP-Server testen und eine Test-E-Mail senden möchten. BlackBerry UEM sendet die Nachricht an die von Ihnen im Feld **Absenderadresse** angegebene E-Mail-Adresse.

Konfigurieren der Datenbankspiegelung

Sie können die Datenbankspiegelung verwenden, um hohe Verfügbarkeit für die BlackBerry UEM-Datenbank zu gewährleisten. Die Datenbankspiegelung ist eine Microsoft SQL Server-Funktion, die Ihnen ermöglicht, den Datenbankdienst und die Datenintegrität aufrechtzuerhalten, wenn Probleme mit der BlackBerry UEM-Datenbank auftreten. Weitere Informationen zur Nutzung von Datenbankspiegelung finden Sie in der Dokumentation zur Planung.

Hinweis: Microsoft plant die Einstellung der Datenbankspiegelung in zukünftigen Versionen von Microsoft SQL Server und empfiehlt stattdessen den Einsatz der AlwaysOn-Funktion für die Konfiguration hoher Verfügbarkeit bei Datenbanken. Für den Einsatz von AlwaysOn sind vor der Installation von BlackBerry UEM Konfigurationsschritte erforderlich. Weitere Informationen zur Nutzung von AlwaysOn finden Sie in der Dokumentation zur Planung. AlwaysOn kann nicht verwendet werden, wenn Sie ein Upgrade von BES5 auf BlackBerry UEM durchführen (d. h. ein Upgrade der BES5-Datenbank auf eine BlackBerry UEM-Datenbank). AlwaysOn wird nicht für Komponenten unterstützt, die BlackBerry OS-Geräte verwalten.

Schritte zum Konfigurieren der Datenbankspiegelung

Führen Sie die folgenden Aktionen aus, um die Datenbankspiegelung zu konfigurieren:

Schritt	Aktion
1	Überprüfen Sie die Anforderungen in der Dokumentation zur Planung, und vergewissern Sie sich, dass die BlackBerry UEM-Domäne die Voraussetzungen erfüllt.
2	Erstellen Sie eine Spiegeldatenbank, starten Sie eine Spiegelungssitzung, und richten Sie einen Zeugenserver ein.
3	Konfigurieren Sie die jeweilige BlackBerry UEM-Instanz, die eine Verbindung zur Spiegeldatenbank herstellt.

Voraussetzungen: Konfigurieren der Datenbankspiegelung

- Konfigurieren Sie den Prinzipalserver und den Spiegelserver so, dass der Zugriff von Remote-Computern zulässig ist.
- Konfigurieren Sie den Prinzipalserver und den Spiegelserver so, dass sie die gleichen Berechtigungen aufweisen.
- Richten Sie einen Zeugenserver ein, der für die Überwachung des Prinzipalservers verwendet wird.
- Konfigurieren Sie den Microsoft SQL Server-Agent so, dass ein Domänenbenutzerkonto mit den gleichen lokalen Administratorrechten wie für das Windows-Konto verwendet wird, das die BlackBerry UEM-Dienste ausführt.
- Vergewissern Sie sich, dass das Domänenbenutzerkonto Berechtigungen für den Prinzipal- und den Spiegelserver aufweist.
- Vergewissern Sie sich, dass der DNS-Server ausgeführt wird.
- Deaktivieren Sie auf jedem Computer, der eine BlackBerry UEM-Datenbankinstanz hostet, im SQL Server 2012 Native Client die Option „Named Pipes“. Wenn Sie die Option „Named Pipes“ nicht deaktivieren möchten, lesen Sie Artikel 34373 unter https://support.blackberry.com/community.

- Informationen zu zusätzlichen Voraussetzungen, die die Microsoft SQL Server-Version Ihres Unternehmens erfüllen muss, finden Sie unter technet.microsoft.com/sqlserver im Artikel Datenbankspiegelung - SQL Server 2012 oder Datenbankspiegelung - SQL Server 2014.
- Wenn die Spiegeldatenbank die standardmäßige Instanz verwendet, können die BlackBerry UEM-Komponenten eine Verbindung mit dieser nur über den standardmäßigen Port 1433, nicht aber über einen benutzerdefinierten statischen Port herstellen. Dies wird bedingt durch eine Einschränkung von Microsoft SQL Server 2005 und höher. Weitere Informationen hierzu finden Sie unter SQL 2005 JDBC Driver and Database Mirroring.

Erstellen und Konfigurieren einer Spiegeldatenbank

Bevor Sie beginnen: Zur Pflege der Datenbankintegrität während der Erstellung und Konfiguration der Spiegeldatenbank sollten die BlackBerry UEM-Dienste auf allen Computern, die eine BlackBerry UEM-Instanz hosten, heruntergefahren werden.

1. Navigieren Sie in Microsoft SQL Server Management Studio zur Prinzipaldatenbank.
2. Ändern Sie die Eigenschaft **Wiederherstellungsmodell** in **VOLLSTÄNDIG**.
3. Führen Sie im Abfrageeditor die Abfrage **-- ALTER DATABASE** *<BUEM_db>* **SET TRUSTWORTHY ON** aus, wobei *<BUEM_db>* der Name der Prinzipaldatenbank ist.
4. Erstellen Sie eine Sicherungskopie der Prinzipaldatenbank. Ändern Sie die Option **Art der Sicherungskopie** in **Vollständig**.
5. Kopieren Sie die Sicherungsdateien auf den Spiegelserver.
6. Stellen Sie die Datenbank auf dem Spiegelserver wieder her, um die Spiegeldatenbank zu erstellen. Wählen Sie beim Wiederherstellen der Datenbank die Option **KEINE NOTFALLWIEDERHERSTELLUNG**.
7. Vergewissern Sie sich, dass der Name der Spiegeldatenbank mit dem Namen der Prinzipaldatenbank übereinstimmt.
8. Klicken Sie auf dem Prinzipalserver in Microsoft SQL Server Management Studio mit der rechten Maustaste auf die Prinzipaldatenbank, und wählen Sie den Task **Spiegeln** aus. Klicken Sie auf der Seite **Spiegelung** auf **Sicherheit konfigurieren**, um den Assistenten zum Konfigurieren der Sicherheit für die Datenbankspiegelung zu starten.
9. Starten Sie die Spiegelung. Weitere Informationen finden Sie unter Einrichten der Datenbankspiegelung – SQL Server 2012 oder Einrichten der Datenbankspiegelung – SQL Server 2014.
10. Fügen Sie der Spiegelungssitzung einen Zeugen hinzu, um die automatische Ausfallsicherung zu aktivieren. Weitere Informationen finden Sie unter Datenbank-Spiegelungszeuge – SQL Server 2012 oder Datenbank-Spiegelungszeuge – SQL Server 2014.

Wenn Sie fertig sind:

- Um sich zu vergewissern, dass die Ausfallsicherung richtig funktioniert, führen Sie manuell eine Ausfallsicherung zur Spiegeldatenbank und zurück zur Prinzipaldatenbank durch.
- Starten Sie die BlackBerry UEM-Dienste auf jedem Computer, der eine BlackBerry UEM-Instanz hostet, neu. Beenden Sie BlackBerry UEM - BlackBerry Work Connect Notification Service nicht zum Ausführen eines Neustarts. Dieser Dienst wird beim Neustart des BlackBerry UEM - BlackBerry Affinity Manager-Diensts automatisch neu gestartet.
- Herstellen der Verbindung von BlackBerry UEM zur Spiegeldatenbank.

Herstellen der Verbindung von BlackBerry UEM zur Spiegeldatenbank

Sie müssen diesen Schritt auf jedem Computer wiederholen, auf dem eine BlackBerry UEM-Instanz gehostet wird. Wenn der BlackBerry Router als einzige BlackBerry UEM-Komponente auf einem Computer vorhanden ist, müssen Sie diesen Schritt auf diesem Computer nicht ausführen.

Bevor Sie beginnen:

- Erstellen und Konfigurieren einer Spiegeldatenbank.
- Vergewissern Sie sich, dass der Spiegelserver ausgeführt wird.
- Sie können diese Aufgabe mithilfe des BlackBerry UEM-Konfigurationstools durchführen, oder Sie können die Datei mit den Datenbankeigenschaften manuell mithilfe der folgenden Anweisungen aktualisieren. Wenn Sie das BlackBerry UEM-Konfigurationstool verwenden möchten, lesen Sie den Artikel KB36443 unter support.blackberry.com/community. Befolgen Sie die Anweisungen im Abschnitt „Aktualisieren der BlackBerry UEM-Datenbankeigenschaften“, um die SQL-Spiegelung zu aktivieren und den FQDN des Spiegelservers bereitzustellen.

1. Navigieren Sie auf dem Computer, auf dem die BlackBerry UEM-Instanz gehostet wird, zu *<Laufwerk>*:\Programme\BlackBerry\UEM\common-settings.
2. Öffnen Sie **DB.properties** in einem Texteditor.
3. Geben Sie im Abschnitt **Optionale Einstellungen für die Verwendung der Ausfallsicherung** nach **configuration.database.ng.failover.server=** den FQDN des Spiegelservers ein (z. B. `configuration.database.ng.failover.server=mirror_server.domain.net`).
4. Falls erforderlich, führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie während der Installation eine benannte Instanz für die Prinzipaldatenbank festgelegt haben, die Spiegeldatenbank jedoch die Standardinstanz verwendet, löschen Sie den Wert nach **configuration.database.ng.failover.instance=**.
   - Wenn die Prinzipaldatenbank eine Standardinstanz und die Spiegeldatenbank eine benannte Instanz verwendet, geben Sie nach **configuration.database.ng.failover.instance=** die benannte Instanz ein.
5. Speichern und schließen Sie **DB.properties**.

Wenn Sie fertig sind:

- Starten Sie die BlackBerry UEM-Dienste neu. Beenden Sie BlackBerry UEM – BlackBerry Work Connect Notification Service nicht zum Ausführen eines Neustarts. Dieser Dienst wird beim Neustart des BlackBerry UEM – BlackBerry Affinity Manager-Diensts automatisch neu gestartet.
- Wiederholen Sie diesen Schritt auf jedem Computer, der eine BlackBerry UEM-Instanz hostet.
- Überprüfen Sie, ob jeder Computer, auf dem eine Instanz von BlackBerry UEM gehostet wird, mithilfe des Serverkurznamens eine Verbindung zum Spiegelserver herstellen kann.

Konfigurieren einer neuen Spiegeldatenbank

Wenn Sie eine neue Spiegeldatenbank erstellen und konfigurieren nachdem ein Rollentausch stattgefunden hat (d. h. die BlackBerry UEM-Komponenten wurden im Zuge der Ausfallsicherung von der vorhandenen Spiegeldatenbank übernommen und die vorhandene Spiegeldatenbank wurde zur Prinzipaldatenbank), wiederholen Sie den Schritt Herstellen der Verbindung von BlackBerry UEM zur Spiegeldatenbank auf jedem Computer, auf dem eine BlackBerry UEM-Instanz gehostet wird.

Konfigurieren Sie ggf. die Komponenten, die BlackBerry OS-Geräte für die Verbindung mit dem neuen Spiegelserver verwalten (siehe Datenbank mit hoher Verfügbarkeit für Komponenten zur Verwaltung von BlackBerry OS-Geräten).

Verbinden von BlackBerry UEM mit Microsoft Azure

Microsoft Azure ist der Microsoft-Cloud-Computing-Service für die Bereitstellung und Verwaltung von Anwendungen und Services. Sie müssen BlackBerry UEM mit Azure verbinden, wenn Sie BlackBerry UEM zur Bereitstellung von iOS- und Android-Apps verwenden möchten, die mit Microsoft Intune verwaltet werden, oder wenn Sie Windows 10-Apps in BlackBerry UEM verwalten möchten.

BlackBerry UEM unterstützt nur die Konfiguration eines Azure-Mandanten. Führen Sie die folgenden Aktionen aus, um BlackBerry UEM mit Azure zu verbinden:

Schritt	Aktion
1	Erstellen eines Microsoft Azure-Kontos.
2	Synchronisieren von Microsoft Active Directory mit Microsoft Azure.
3	Erstellen eines Unternehmensendpunkts in Azure.
4	Konfigurieren Sie BlackBerry UEM für die Synchronisierung mit Microsoft Intune und Windows Store für Unternehmen.

Erstellen eines Microsoft Azure-Kontos

Für die Bereitstellung von durch Microsoft Intune geschützte Apps für iOS- und Android-Geräte oder für das Verwalten von Windows 10-Apps in BlackBerry UEM, müssen Sie über ein Microsoft Azure-Konto verfügen und BlackBerry UEM über Azure authentifizieren.

Führen Sie diese Aufgabe durch, wenn Ihre Organisation nicht über ein Microsoft Azure-Konto verfügt.

Hinweis: Um sicherzustellen, dass Sie über die richtigen Lizenzen und Kontoberechtigungen für Microsoft Intune verfügen, lesen Sie Artikel 50341 unter support.blackberry.com/community.

1. Gehen Sie zu https://azure.microsoft.com, klicken Sie auf **Kostenloses Konto**, und befolgen Sie dann die Anweisungen, um das Konto zu erstellen.

   Zum Erstellen des Kontos müssen Sie Kreditkarteninformationen angeben.
2. Registrieren Sie sich beim Azure-Verwaltungsportal unter https://portal.azure.com, und melden Sie sich mit dem bei der Registrierung erstellten Benutzernamen und Kennwort an.

Wenn Sie fertig sind: Synchronisieren von Microsoft Active Directory mit Microsoft Azure.

Synchronisieren von Microsoft Active Directory mit Microsoft Azure

Um Windows 10-Benutzern die Installation von Online-Apps oder das Senden von Apps zu erlauben, die durch Microsoft Intune- iOS- und Android-Geräte geschützt sind, müssen die Benutzer in Microsoft AzureActive Directory vorhanden sein. Sie Benutzer und Gruppen zwischen Ihrem lokalen Active Directory und AzureActive Directory mithilfe von Microsoft Azure Active Directory Connect synchronisieren. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect.

Bevor Sie beginnen: Erstellen eines Microsoft Azure-Kontos

1. Laden Sie Azure AD Connect von http://www.microsoft.com/en-us/download/details.aspx?id=47594 herunter.
2. Installieren Sie die Azure AD Connect-Software.
3. Konfigurieren Sie Azure AD Connect für die Verbindung mit Ihrem firmeninternen Active Directory mit dem AzureActive Directory.

Wenn Sie fertig sind: Erstellen eines Unternehmensendpunkts in Azure

Erstellen eines Unternehmensendpunkts in Azure

Um BlackBerry UEM-Zugriff auf Microsoft Azure bereitzustellen, müssen Sie einen Unternehmensendpunkt innerhalb von Azure erstellen. Der Unternehmensendpunkt ermöglicht es BlackBerry UEM, sich bei Microsoft Azure zu authentifizieren. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration.

Wenn Sie BlackBerry UEM mit Microsoft Intune und Windows Store für Unternehmen verbinden, verwenden Sie eine andere Unternehmensanwendung für jeden Zweck aufgrund von Unterschieden bei den Berechtigungen und möglichen zukünftigen Änderungen.

Bevor Sie beginnen: Synchronisieren von Microsoft Active Directory mit Microsoft Azure

1. melden Sie sich beim Azure-Portal an.
2. Navigieren Sie zu **Microsoft Azure > Azure Active Directory > App-Registrierungen**.
3. Klicken Sie auf **Endpunkte**.
4. Kopieren Sie den Wert unter **OAuth 2.0-Token-Endpunkt (v1)**, und fügen Sie ihn in eine Textdatei ein.
   Dies ist der **OAuth 2.0-Token-Endpunkt**, der in BlackBerry UEM erforderlich ist.
5. Schließen Sie die Liste **Endpunkte**, und klicken Sie auf **+Neue Registrierung**.
6. Geben Sie einen Namen für Ihre App ein.
7. Wählen Sie aus, welche Kontotypen die Anwendung verwenden oder auf die API zugreifen können.
8. Klicken Sie auf **Registrieren**.
9. Kopieren Sie die **Anwendungs-ID** Ihrer Anwendung, und fügen Sie sie in eine Textdatei ein.
   Dies ist die **Client-ID**, die in BlackBerry UEM erforderlich ist.
10. Wenn Sie die Anwendung zur Verwendung von Microsoft Intune erstellen, klicken Sie auf **API-Berechtigungen** im Abschnitt **Verwalten**. Führen Sie folgende Schritte aus:
    a) Klicken Sie auf **+Berechtigung hinzufügen**.
    b) Wählen Sie **Microsoft Graph**.
    c) Wählen Sie **Delegierte Berechtigungen** aus.
    d) Blättern Sie in der Liste der Berechtigungen nach unten, und legen Sie unter **Delegierte Berechtigungen** die folgenden Berechtigungen für Microsoft Intune fest:
       - Microsoft Intune-Apps lesen und schreiben (**DeviceManagementApps > DeviceManagementApps.ReadWrite.All**)
       - Alle Gruppen lesen (**Gruppe > Group.Read.All**)
       - Basisprofil aller Benutzer lesen (**Benutzer > User.ReadBasic.All**)
    e) Klicken Sie auf **Berechtigung hinzufügen**.
    f) Klicken Sie unter **Einwilligung erteilen** auf **Administratoreinwilligung erteilen**.

       Hinweis: Nur globale Administratoren können Berechtigungen gewähren.
    g) Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**, um die Berechtigungen für alle Konten im aktuellen Verzeichnis zu gewähren.

Sie können die Standardberechtigungen verwenden, wenn Sie die App zum Verbinden mit Windows Store for Business erstellen.

11. Klicken Sie im Abschnitt **Verwalten** auf **Zertifikate und Schlüssel**. Führen Sie folgende Schritte aus:
    a) Klicken Sie unter **Client-Schlüssel** auf **+Neuer Client-Schlüssel**.
    b) Geben Sie eine Beschreibung für den Client-Schlüssel ein.
    c) Wählen Sie eine Dauer für den Client-Schlüssel aus.
    d) Klicken Sie auf **Hinzufügen**.
    e) Kopieren Sie den Wert des neuen Client-Schlüssels.

    Dies ist der **Client-Schlüssel**, der in BlackBerry UEM erforderlich ist.

    Warnung: Wenn Sie den Wert Ihres Schlüssels zu diesem Zeitpunkt nicht kopieren, müssen Sie einen neuen Schlüssel erstellen, da der Wert nicht angezeigt wird, nachdem Sie diesen Bildschirm verlassen.

Wenn Sie fertig sind: Konfigurieren von BlackBerry UEM für die Synchronisierung mit Microsoft Intune oder Konfigurieren von BlackBerry UEM für die Synchronisierung mit dem Windows Store for Business.

Aktivierung des Zugriffs auf BlackBerry Web Services über den BlackBerry Infrastructure

Wenn Ihr Unternehmen einen Webservice-Client verwendet, der sich außerhalb der Firewall des Unternehmens befindet, und der Client Zugriff auf die APIs der BlackBerry Web Services (REST oder alte SOAP-APIs) benötigt, kann er über den BlackBerry Infrastructure eine Verbindung zu ihnen herstellen. Weitere Informationen zur Aktivierung dieses Zugriffs in Client-Apps finden Entwickler im Abschnitt „Erste Schritte“ des Referenzmaterials für REST-APIs der BlackBerry Web Services.

Webservice-Clients können den BlackBerry Infrastructure nur dann zum Zugriff auf BlackBerry Web Services-APIs verwenden, wenn diese Zugriffsmöglichkeit in der Verwaltungskonsole aktiviert wurde. Standardmäßig ist diese Option deaktiviert.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Zugriff auf BlackBerry Web Services**.
2. Klicken Sie auf **Aktivieren**.
3. Klicken Sie auf **Speichern**.

Abrufen eines APNs-Zertifikats für die Verwaltung von iOS- und macOS-Geräten

APNs ist der Apple Push Notification Service. Sie müssen das APNs-Zertifikat abrufen und registrieren, wenn Sie BlackBerry UEM für die Verwaltung von iOS- oder macOS-Geräten verwenden möchten. Wenn Sie mehr als eine BlackBerry UEM-Domäne einrichten, ist für jede Domäne ein APNs-Zertifikat erforderlich.

APNs-Zertifikate können mithilfe des Assistenten für die erstmalige Anmeldung oder unter Verwendung des Abschnitts „Externe Integration“ der Verwaltungskonsole abgerufen und registriert werden.

Hinweis: Jedes APNs-Zertifikat ist ein Jahr lang gültig. Auf der Verwaltungskonsole wird das Ablaufdatum angezeigt. Sie müssen das APNs-Zertifikat vor dem Ablaufdatum erneuern. Verwenden Sie hierzu die Apple-ID, die Sie zum Abrufen des Zertifikats benötigen. Sie können eine E-Mail Ereignisbenachrichtigung erstellen, um Sie daran zu erinnern, das Zertifikat 30 Tage vor Ablauf zu erneuern. Wenn das Zertifikat abläuft, empfangen Geräte von BlackBerry UEM keine Daten mehr. Wenn Sie ein neues APNs-Zertifikat registrieren, müssen Benutzer ihre Geräte neu aktivieren, um Daten zu empfangen.

Weitere Informationen finden Sie unter https://developer.apple.com im Artikel TN2265 unter *Issues with Sending Push Notifications*.

In der Praxis hat es sich bewährt, auf die Verwaltungskonsole und das Apple Push Certificates Portal über den Google Chrome-Browser oder den Safari-Browser zuzugreifen. Diese Browser bieten optimale Unterstützung bei der Anforderung und Registrierung von APNs-Zertifikaten.

Führen Sie zum Abrufen und Registrieren eines APNs-Zertifikats die folgenden Aktionen aus:

Schritt	Aktion
1	Rufen Sie eine signierte CSR von BlackBerry ab.
2	Fordern Sie mit der signierten CSR-Datei ein APNs-Zertifikat von Apple an.
3	Registrieren Sie das APNs-Zertifikat.

Abrufen einer signierten CSR-Datei von BlackBerry

Sie müssen eine signierte CSR-Datei (Certificate Signing Request) von BlackBerry abrufen, bevor Sie ein APNs-Zertifikat anfordern können.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie auf **APNs-Zertifikat abrufen**.

   Wenn Sie ein aktuell verwendetes APNs-Zertifikat erneuern möchten, klicken Sie stattdessen auf **Zertifikat erneuern**.
3. Klicken Sie im Abschnitt **Schritt 1 von 3 – Signiertes CSR-Zertifikat von BlackBerry herunterladen** auf **Zertifikat herunterladen**.
4. Klicken Sie auf **Speichern**, um die signierte CSR-Datei (.scsr) auf Ihrem Computer zu speichern.

Wenn Sie fertig sind: Anfordern eines APNs-Zertifikats von Apple.

Anfordern eines APNs-Zertifikats von Apple

Bevor Sie beginnen: Abrufen einer signierten CSR-Datei von BlackBerry.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie im Abschnitt **Schritt 2 von 3 – APNs-Zertifikat von Apple anfordern** auf **Apple Push Certificates Portal**. Sie werden zum Apple Push Certificates Portal weitergeleitet.
3. Melden Sie sich beim Apple Push Certificates Portal mit einer gültigen Apple-ID an.
4. Befolgen Sie die Anweisungen zum Hochladen der signierten CSR-Datei (.scsr).
5. Laden Sie das APNs-Zertifikat (.pem) auf Ihren Computer herunter, und speichern Sie es.

Wenn Sie fertig sind: Registrieren des APNs-Zertifikats.

Registrieren des APNs-Zertifikats

Bevor Sie beginnen: Anfordern eines APNs-Zertifikats von Apple.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie im Abschnitt **Schritt 3 von 3 – APNs-Zertifikat registrieren** auf **Durchsuchen**. Navigieren Sie zum APNs-Zertifikat (.pem), und wählen Sie es aus.
3. Klicken Sie auf **Submit**.

Wenn Sie fertig sind:

- Zum Testen der Verbindung zwischen BlackBerry UEM und dem APNs-Server klicken Sie auf **APNS-Zertifikat testen**.
- Um den Status und das Ablaufdatum des APNs-Zertifikats anzuzeigen, klicken Sie auf **Einstellungen > Externe Integration > iOS-Verwaltung**. Weitere Informationen zur Erneuerung von APNs-Zertifikaten finden Sie unter Erneuern des APNs-Zertifikats.

Erneuern des APNs-Zertifikats

Das APNs-Zertifikat ist ein Jahr lang gültig. Sie müssen das APNs-Zertifikat jährlich vor dem Ablaufdatum erneuern.

Sie können eine E-Mail Ereignisbenachrichtigung erstellen, um Sie daran zu erinnern, das Zertifikat 30 Tage vor Ablauf zu erneuern.

Bevor Sie beginnen: Abrufen einer signierten CSR-Datei von BlackBerry.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie im Abschnitt **Schritt 2 von 3 – APNs-Zertifikat von Apple anfordern** auf **Apple Push Certificates Portal**. Sie werden zum Apple Push Certificates Portal weitergeleitet.
3. Melden Sie sich beim Apple Push Certificates Portal mit derselben Apple-ID an, die Sie zum Abrufen des ursprünglichen APNs-Zertifikats verwendet haben.
4. Befolgen Sie die Anweisungen zum Erneuern des APNs-Zertifikats (.pem). Sie müssen die neue signierte CSR hochladen.
5. Laden Sie das erneuerte APNs-Zertifikat auf Ihren Computer herunter, und speichern Sie es.
6. Klicken Sie im Abschnitt **Schritt 3 von 3 – APNs-Zertifikat registrieren** auf **Durchsuchen**. Navigieren Sie zu dem erneuerten APNs-Zertifikat, und wählen Sie es aus.

7. Klicken Sie auf **Senden**.

Wenn Sie fertig sind:

- Zum Testen der Verbindung zwischen BlackBerry UEM und dem APNs-Server klicken Sie auf **APNs-Zertifikat testen**.
- Um den Status und das Ablaufdatum des APNs-Zertifikats anzuzeigen, klicken Sie auf **Einstellungen > Externe Integration > iOS-Verwaltung**.

Fehlerbehebung: APNs

Dieser Abschnitt hilft Ihnen bei der Behebung von APNs-Problemen.

Das APNs-Zertifikat stimmt nicht mit der CSR überein. Stellen Sie die korrekte APNs-Datei (.pem) bereit, oder senden Sie eine neue CSR.

Beschreibung

Möglicherweise wird eine Fehlermeldung angezeigt, wenn Sie versuchen, ein APNs-Zertifikat zu registrieren und die neueste signierte CSR-Datei nicht von BlackBerry auf das Apple Push Certificates Portal hochgeladen haben.

Mögliche Lösung

Wenn Sie mehrere CSR-Dateien von BlackBerry heruntergeladen haben, ist nur die letzte heruntergeladene Datei gültig. Wenn Sie wissen, welche CSR die aktuellste ist, kehren Sie zum Apple Push Certificates Portal zurück, und laden Sie sie hoch. Wenn Sie nicht sicher sind, welche CSR die aktuellste ist, rufen Sie eine neue von BlackBerry ab. Kehren Sie dann zum Apple Push Certificates Portal zurück und laden Sie sie hoch.

Beim Abrufen einer signierten CSR erhalte ich die Meldung „Im System ist ein Fehler aufgetreten“

Beschreibung

Beim Versuch, eine signierte CSR abzurufen, erhalten Sie folgende Fehlermeldung: „Im System ist ein Fehler aufgetreten. Versuchen Sie es erneut.“

Mögliche Lösung

Gehen Sie zu http://support.blackberry.com/kb, um Artikel KB37266 zu lesen.

Ich kann iOS- oder macOS-Geräte nicht aktivieren

Problemursache

Wenn Sie iOS- oder macOS-Geräte nicht aktivieren können, wurde das APNs-Zertifikat möglicherweise nicht ordnungsgemäß registriert.

Mögliche Lösung

Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Apple Push Notification**. Vergewissern Sie sich, dass das APNs-Zertifikat den Status „Installiert“ aufweist. Wenn der Status nicht korrekt ist, versuchen Sie, das APNs-Zertifikat erneut zu registrieren.
- Klicken Sie auf **APNS-Zertifikat testen**, um die Verbindung zwischen BlackBerry UEM und dem APNs-Server zu testen.
- Rufen Sie ggf. eine neue signierte CSR von BlackBerry und ein neues APNs-Zertifikat ab.

Konfigurieren von BlackBerry UEM für DEP

Sie müssen BlackBerry UEM für die Verwendung des Programms zur Geräteregistrierung (DEP) von Apple konfigurieren, damit Sie BlackBerry UEM mit DEP synchronisieren können. Nach der Konfiguration von BlackBerry UEM können Sie die Aktivierung der von Ihrem Unternehmen für DEP erworbenen iOS-Geräte mit der BlackBerry UEM-Verwaltungskonsole verwalten.

Sie können ein Apple Business Manager-Konto für die Synchronisation von BlackBerry UEM mit DEP verwenden. Apple Business Manager ist ein Web-basiertes Portal, in dem Sie iOS-Geräte in DEP registrieren und verwalten können. Außerdem ist darin die Verwaltung von Apple VPP-Konten möglich. Wenn Ihre Organisation DEP oder VPP verwendet, können Sie auf Apple Business Manager aktualisieren.

Beim Konfigurieren von BlackBerry UEM für das Programm zur Geräteregistrierung von Apple führen Sie die folgenden Schritte aus:

Schritt	Aktion
1	Erstellen eines DEP-Kontos.
2	Herunterladen eines öffentlichen Schlüssels.
3	Generieren eines Server-Tokens.
4	Registrieren des Server-Tokens bei BlackBerry UEM.
5	Hinzufügen der ersten Registrierungskonfiguration.

Erstellen eines DEP-Kontos

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf +.
3. Geben Sie im Feld **Name** einen Namen für das Konto ein.
4. Klicken Sie in **Schritt 1 von 4: Erstellen eines Apple DEP-Kontos** auf **Erstellen eines Apple DEP-Kontos**.
5. Füllen Sie die Felder aus, und befolgen Sie die Anweisungen zum Erstellen des Kontos.

Wenn Sie fertig sind: Herunterladen eines öffentlichen Schlüssels.

Herunterladen eines öffentlichen Schlüssels

Bevor Sie beginnen: Erstellen eines DEP-Kontos.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf +.
3. Klicken Sie in Schritt **2 von 4: Herunterladen eines öffentlichen Schlüssels auf Herunterladen des öffentlichen Schlüssels**.
4. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Generieren eines Server-Tokens.

Generieren eines Server-Tokens

Bevor Sie beginnen: Herunterladen eines öffentlichen Schlüssels.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf +.
3. Klicken Sie in **Schritt 3 von 4: Erzeugen eines Server-Tokens aus dem Apple DEP-Konto** auf **Öffnen des DEP-Portals von Apple**.
4. Melden Sie sich bei Ihrem DEP-Konto an.
5. Befolgen Sie die Anweisungen zum Generieren eines Server-Tokens.

Wenn Sie fertig sind: Registrieren des Server-Tokens bei BlackBerry UEM.

Registrieren des Server-Tokens bei BlackBerry UEM

BlackBerry UEM verwendet bei der Kommunikation mit dem Programm zur Geräteregistrierung von Apple ein Server-Token zur Authentifizierung.

Bevor Sie beginnen: Generieren eines Server-Tokens.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf +.
3. Klicken Sie in **Schritt 4 von 4: Registrieren des Server-Tokens bei BlackBerry UEM** auf **Durchsuchen**.
4. Wählen Sie die Server-Token-Datei mit der Erweiterung **.p7m** aus.
5. Klicken Sie auf **Öffnen**.
6. Klicken Sie auf **Weiter**.

Wenn Sie fertig sind: Hinzufügen der ersten Registrierungskonfiguration.

Hinzufügen der ersten Registrierungskonfiguration

Bevor Sie beginnen: Registrieren des Server-Tokens bei BlackBerry UEM bevor Sie Ihre erste Registrierungskonfiguration hinzufügen.

Nachdem Sie ein Server-Token registriert haben, wird in BlackBerry UEM automatisch das Fenster zum Hinzufügen der ersten Registrierungskonfiguration angezeigt.

1. Geben Sie einen Namen für die Konfiguration ein.

2. Führen Sie eine der folgenden Aufgaben aus:
   - Wenn Sie möchten, dass BlackBerry UEM Geräten bei der Registrierung im Apple-Programm zur Geräteregistrierung automatisch die Registrierungskonfiguration zuweist, aktivieren Sie das Kontrollkästchen „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“.
   - Wenn Sie die BlackBerry UEM-Konsole verwenden möchten, um die Registrierungskonfiguration manuell bestimmten Geräten zuzuweisen, deaktivieren Sie das Kontrollkästchen „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“.
3. Geben Sie optional einen Abteilungsnamen und eine Supporttelefonnummer ein, die während der Einrichtung auf Geräten angezeigt werden sollen.
4. Treffen Sie im Abschnitt **Gerätekonfiguration** Ihre Auswahl aus folgenden Kontrollkästchen:
   - Kopplung zulassen: Wenn diese Option aktiviert ist, können Benutzer das Gerät mit einem Computer koppeln.
   - Beaufsichtigten Modus aktivieren: Wenn diese Option aktiviert ist, werden Geräte im beaufsichtigten Modus aktiviert. Sie müssen „Beaufsichtigten Modus aktivieren“ und/oder „Entfernen des MDM-Profils zulassen“ auswählen.
   - Erforderlich: Wenn diese Option ausgewählt ist, können Benutzer Geräte mit ihrem Unternehmensbenutzernamen und -kennwort aktivieren.
   - Entfernen des MDM-Profils zulassen: Wenn diese Option aktiviert ist, können Benutzer Geräte deaktivieren. Sie müssen „Beaufsichtigten Modus aktivieren“ und/oder „Entfernen des MDM-Profils zulassen“ auswählen.
   - Warten, bis das Gerät konfiguriert wurde: Wenn diese Option aktiviert ist, können Benutzer die Geräteeinrichtung nicht abbrechen, bevor die Aktivierung in BlackBerry UEM abgeschlossen wurde. Diese Einstellung ist nur gültig, wenn Sie „Beaufsichtigten Modus aktivieren“ ausgewählt haben.
5. Wählen Sie im Abschnitt **Bei der Einrichtung überspringen** die Elemente aus, die nicht in der Geräteeinrichtung enthalten sein sollen:
   - Kennung: Wenn diese Option aktiviert ist, werden Benutzer nicht aufgefordert, eine Gerätekennung zu erstellen.
   - Standortbestimmung: Wenn diese Option aktiviert ist, sind die Standortbestimmungsdienste auf dem Gerät deaktiviert.
   - Wiederherstellen: Wenn diese Option aktiviert ist, können Benutzer keine Daten aus einer Sicherungsdatei wiederherstellen.
   - Von Android migrieren: Wenn diese Option ausgewählt ist, können Sie keine Daten von einem Android-Gerät wiederherstellen.
   - Apple ID: Wenn diese Option aktiviert ist, können Benutzer sich nicht bei Apple ID und iCloud anmelden.
   - Geschäftsbedingungen: Wenn diese Option aktiviert ist, werden Benutzern die iOS Geschäftsbedingungen nicht angezeigt.
   - Siri: Wenn diese Option ausgewählt ist, ist Siri auf Geräten deaktiviert.
   - Diagnose: Wenn diese Option aktiviert ist, werden Diagnoseinformationen während der Einrichtung nicht automatisch vom Gerät gesendet.
   - Biometrisch: Wenn diese Option ausgewählt ist, können Benutzer keine Touch-ID einrichten.
   - Zahlung: Wenn diese Option aktiviert ist, können Benutzer Apple Pay nicht einrichten.
   - Zoom: Wenn diese Option ausgewählt ist, können Benutzer Zoom nicht einrichten.
   - Einrichtung der Home-Taste – Wenn diese Option ausgewählt ist, können Benutzer den Klick der Home-Taste nicht anpassen
   - Bildschirmzeit: Wenn diese Option ausgewählt ist, wird die Option zum Einrichten der Bildschirmzeit während der DEP-Registrierung übersprungen.
   - Softwareupdate: Wenn diese Option ausgewählt ist, wird dem Benutzer der Bildschirm für obligatorische Softwareupdates auf dem Gerät nicht angezeigt.

- iMessage und Face Time: Wenn diese Option ausgewählt ist, wird der Bildschirm iMessage und Face Time auf dem Gerät nicht angezeigt.

6. Klicken Sie auf **Speichern**.

   Wenn die Meldung „Ein Fehler ist aufgetreten. Die Server-Token-Datei konnte nicht entschlüsselt werden.“ angezeigt wird, lesen Sie Artikel 37282 unter support.blackberry.com/community.
7. Wenn Sie die Option „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“ ausgewählt haben, klicken Sie auf **Ja**.

Wenn Sie fertig sind: Aktivieren Sie iOS-Geräte. Weitere Informationen zur Aktivierung von Geräten, die bei DEP registriert sind, finden Sie in der Dokumentation für Administratoren.

Aktualisieren des Server-Tokens

Das Server-Token ist ein Jahr lang gültig. Sie müssen das Token jährlich vor dem Ablaufdatum erneuern. Den Status des Tokens finden Sie unter dem „Ablaufdatum“ im Programm zur Geräteregistrierung von Apple.

Bevor Sie beginnen: Wenn der öffentliche Schlüssel geändert wurde, laden Sie einen neuen öffentlichen Schlüssel herunter.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf den Namen des DEP-Kontos.
3. Klicken Sie im Bereich **Ablaufdatum** auf **Server-Token aktualisieren** .
4. Klicken Sie in **Schritt 1 von 2: Erzeugen eines Server-Tokens aus dem Apple DEP-Konto** auf **Öffnen des DEP-Portals von Apple**.
5. Melden Sie sich bei Ihrem DEP-Konto an.
6. Befolgen Sie die Anweisungen zum Generieren eines Server-Tokens.
7. Klicken Sie in **Schritt 2 von 2: Registrieren des Server-Tokens bei BlackBerry UEM** auf **Durchsuchen**.
8. Wählen Sie die Server-Token-Datei mit der Erweiterung **.p7m** aus.
9. Klicken Sie auf **Öffnen**.
10. Klicken Sie auf **Speichern**.

Entfernen einer DEP-Verbindung

VORSICHT: Wenn Sie alle DEP-Verbindungen entfernen, können Sie keine neuen iOS-Geräte im Geräteregistrierungsprogramm von Apple aktivieren. Wenn Sie Geräten Registrierungskonfigurationen zuweisen und die Konfigurationen nicht angewendet wurden, entfernt BlackBerry UEM die Registrierungskonfigurationen, die den Geräten zugewiesen sind. Das Entfernen der Verbindung wirkt sich nicht auf Geräte aus, die auf BlackBerry UEM aktiviert sind.

Wenn Ihr Unternehmen keine iOS-Geräte mehr bereitstellt, die DEP verwenden, können Sie die BlackBerry UEM-Verbindungen zu DEP entfernen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf den Namen des DEP-Kontos.
3. Klicken Sie auf **DEP-Verbindung entfernen**.
4. Klicken Sie auf **Entfernen**.
5. Klicken Sie auf **OK**.

Konfigurieren von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten

Android Enterprise-Geräte bieten zusätzliche Sicherheit für Unternehmen, die ihre Android-Geräte verwalten möchten. Weitere Informationen zu Android Enterprise-Geräten finden Sie unter https://support.google.com/work/android/.

Ausführliche Anweisungen zur Konfiguration von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten finden Sie im Artikel 37748 unter support.blackberry.com/community.

Hinweis: Sie können Anwendungsrichtlinien verwenden, um die Gmail-App für Android Enterprise-Geräte zu konfigurieren.

Es gibt zwei Möglichkeiten, BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten zu konfigurieren:

1. Stellen Sie eine Verbindung zwischen BlackBerry UEM und einer Google Cloud- oder G Suite-Domäne her.

   Hinweis: Sie können nur eine BlackBerry UEM-Domäne mit einer Google-Domäne verbinden.
2. Lassen Sie zu, dass BlackBerry UEM Android Enterprise-Geräte verwaltet, die über verwaltete Google Play-Konten verfügen. Sie benötigen keine Google-Domäne, um diese Option zu verwenden. Weitere Informationen finden Sie unter https://support.google.com/googleplay/work/.

In der folgenden Tabelle werden die unterschiedlichen Optionen für die Konfiguration von Android Enterprise-Geräten zusammengefasst:

Methode für die Konfiguration von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten	Wann diese Methode verwendet werden sollte	Typ des Benutzerkontos	Unterstützte Google-Dienste
BlackBerry UEM mit Ihrer G Suite-Domäne verbinden	Sie haben eine G Suite-Domäne im Unternehmen	G Suite-Konten (für Unternehmen)	Unterstützt alle G Suite-Dienste, z B. Gmail, Google Calendar und Drive. Unterstützt die App-Verwaltung über Google Play.
BlackBerry UEM mit Ihrer Google Cloud-Domäne verbinden	Sie haben eine Google Cloud-Domäne im Unternehmen	Google Cloud-Konten, die auch als Managed Google-Konten (für Unternehmen) bezeichnet werden	Ähnlich wie G Suite, aber ohne Zugriff auf kostenpflichtige Produkte, z. B. Gmail, Google Calendar und Drive. Unterstützt die App-Verwaltung über Google Play.

Methode für die Konfiguration von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten	Wann diese Methode verwendet werden sollte	Typ des Benutzerkontos	Unterstützte Google-Dienste
Zulassen, dass BlackBerry UEM Android Enterprise-Geräte verwaltet, die über verwaltete Google Play-Konten verfügen	Sie haben keine Google-Domäne im Unternehmen oder Sie haben eine Google-Domäne, die bereits mit einer BlackBerry UEM-Domäne verbunden ist, und möchten Android Enterprise-Geräte in einer zweiten BlackBerry UEM-Domäne nutzen	Android Enterprise-Geräte mit verwalteten Google Play-Konten	Unterstützt die App-Verwaltung über Google Play. Google-Dienste werden nicht unterstützt.

Konfigurieren von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten

Sie können nur eine BlackBerry UEM-Domäne mit der Google-Domäne verbinden. Bevor Sie eine Verbindung mit einer anderen BlackBerry UEM-Domäne herstellen, müssen Sie die bestehende Verbindung entfernen. Siehe Entfernen der Verbindung zu Ihrer Google-Domäne.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Android Enterprise**.
2. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Verwenden von Android Enterprise-Geräten mit verwalteten Google Play-Konten	**a.** Wählen Sie **Zulassen, dass Google Play-Konten durch BlackBerry UEM verwaltet werden**. **b.** Klicken Sie auf **Weiter**. **c.** Melden Sie sich im Fenster **Bring Android to Work** mit einem Google-Konto an. Sie können hierfür ein beliebiges Google- oder Gmail-Konto verwenden. Das von Ihnen verwendete Konto wird zum Administratorkonto für den Dienst **Bring Android to Work**. **d.** Klicken Sie auf **Erste Schritte**. **e.** Geben Sie den Namen Ihres Unternehmens ein. Klicken Sie auf **Bestätigen**. **f.** Klicken Sie auf **Registrierung abschließen**. Die BlackBerry UEM-Verwaltungskonsole wird wieder angezeigt.

Aufgabe	Schritte
Verwenden einer Google-Domäne	a. Wählen Sie **BlackBerry UEM mit Ihrer vorhandenen Google-Domäne verbinden**. b. Klicken Sie auf **Weiter**. c. Füllen Sie die Felder zum Erstellen eines Dienstkontos aus, und klicken Sie auf **Weiter**. Weitere Schritt-für-Schritt-Anleitungen finden Sie unter support.blackberry.com/community in Artikel 37748.

3. Geben Sie an, wie App-Konfigurationen an ein Gerät gesendet werden sollen. Alle Informationen, die Sie in der App-Konfiguration hinzugefügt haben, können entweder über die BlackBerry Infrastructure oder über die Google-Infrastruktur bereitgestellt werden. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie **App-Konfiguration über UEM Client senden** aus, um Informationen der App-Konfiguration über die BlackBerry Infrastructure zu senden.
   - Wählen Sie **App-Konfiguration über Google Play senden**, um Informationen der App-Konfiguration über die Google-Infrastruktur zu senden.
4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Annehmen**, um die Berechtigungen für die folgenden Apps zu akzeptieren:
   - Google Chrome
   - BlackBerry Connectivity
   - BlackBerry Hub +-Dienste
   - BlackBerry Hub
   - BlackBerry-Kalender
   - Kontakte von BlackBerry
   - Notizen von BlackBerry
   - Aufgaben von BlackBerry
5. Klicken Sie auf **Fertig**.

Wenn Sie fertig sind: Schließen Sie die Schritte für die Aktivierung von Android Enterprise-Geräten ab. Weitere Informationen zur Aktivierung von Geräten finden Sie in der Dokumentation für Administratoren unter „Geräteaktivierung“.

Entfernen der Verbindung zu Ihrer Google-Domäne

Sie können nur eine BlackBerry UEM-Domäne mit der Google Cloud- bzw. G Suite-Domäne verbinden. Bevor Sie eine Verbindung mit einer anderen BlackBerry UEM-Domäne herstellen, müssen Sie die bestehende Verbindung entfernen.

Entfernen Sie die Verbindung zu Ihrer Google-Domäne, bevor Sie die folgenden Aufgaben durchführen:

- Deinstallieren einer BlackBerry UEM-Instanz
- Wiederherstellen des Snapshots des virtuellen Computers, den Sie vor der Einrichtung der Verbindung erstellt haben
- Verbinden einer anderen BlackBerry UEM-Instanz mit der Google Cloud- oder G Suite-Domäne

Wenn Sie die Verbindung zu Ihrer Google-Domäne nicht entfernen, können Sie möglicherweise keine Verbindung zwischen der Google Cloud- oder G Suite-Domäne und einer neuen BlackBerry UEM-Instanz herstellen. Wenn Sie die Verbindung in BlackBerry UEM entfernen, deaktivieren Sie damit auch alle Geräte, die mit der Aktivierungsart Android Enterprise aktiviert wurden.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration**.

2. Klicken Sie auf **Google-Domänenverbindung**.
3. Klicken Sie auf **Verbindung entfernen**.
4. Klicken Sie auf **Entfernen**.

Entfernen der Google-Domänenverbindung mithilfe Ihres Google-Kontos

Wenn Sie BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten konfiguriert haben, können Sie die Verbindung in Google entfernen.

1. Melden Sie sich mithilfe des Google-Kontos, das Sie für die Einrichtung von Android Enterprise-Geräten verwendet haben, bei https://play.google.com/work an.
2. Klicken Sie auf **Admin-Einstellungen**.
3. Klicken Sie im Abschnitt **Unternehmensinformationen** auf .
4. Klicken Sie auf **Unternehmen löschen**.
5. Klicken Sie auf **Löschen**.
6. Klicken Sie in der Menüleiste der BlackBerry UEM-Konsole auf **Einstellungen > Externe Integration**.
7. Klicken Sie auf **Google-Domänenverbindung**.
8. Klicken Sie auf **Verbindung testen**.
9. Klicken Sie auf **Verbindung entfernen**.
10. Klicken Sie auf **Entfernen**.

Bearbeiten oder Testen der Google-Domänenverbindung

Sie können die Google-Verbindung in BlackBerry UEM bearbeiten, um den Typ der Google-Domäne zu ändern, den Sie zur Verwaltung von Android Enterprise verwenden, oder um die Google-Verbindung zu testen. Wenn Sie die Verbindung bearbeiten oder testen, sind bereits aktivierte Geräte nicht betroffen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration**.
2. Klicken Sie auf **Google-Domänenverbindung**.
3. Klicken Sie auf .
4. Führen Sie eine der folgenden Aufgaben aus:
   - Klicken Sie auf **Verbindung testen**, um den aktuellen Status der Verbindung anzuzeigen.
   - Wählen Sie zum Verwalten von Android Enterprise-Geräten den Typ der Domäne aus, und klicken Sie auf **Speichern**.

Vereinfachung von Windows 10-Aktivierungen

Sie können eine Java-Webanwendung von BlackBerry als Suchdienst verwenden, um den Aktivierungsvorgang für Benutzer mit Windows 10-Geräten zu vereinfachen. Wenn Sie den Suchdienst verwenden, müssen Sie während des Aktivierungsvorgangs keine Serveradresse eingeben. Wenn Sie diese Webanwendung nicht bereitstellen möchten, können Benutzer Windows 10-Geräte auch aktivieren, indem sie die Serveradresse bei Aufforderung eingeben.

Sie können verschiedene Betriebssysteme und Webanwendungs-Tools zur Bereitstellung einer Suchdienst-Webanwendung verwenden. Dieser Abschnitt beinhaltet die Schritte der oberen Ebene. Unter Bereitstellen eines Suchdienstes zur Vereinfachung von Windows 10-Aktivierungen finden Sie ein Beispiel für die spezifischen Schritte für gängige Betriebssysteme und Tools.

Wenn Sie eine Suchdienst-Webanwendung bereitstellen, führen Sie die folgenden Schritte aus:

Schritt	Aktion
1	Erstellen Sie einen statischen DNS-Host-A-Datensatz für den Java-Anwendungsserver. Der Datensatz muss `enterpriseenrollment.<E-Mail-Domäne>` lauten. Dabei entspricht <*E-Mail-Domäne*> der E-Mail-Adresse der Benutzer.
2	Wenn Sie Benutzern die Berechtigung erteilen möchten, Geräte zu aktivieren, wenn sie sich außerhalb des Unternehmensnetzwerks befinden, konfigurieren Sie den Computer, der den Suchdienst hostet, für den externen Empfang über Port 443.
3	Erstellen und installieren Sie ein Zertifikat, um für sichere TLS-Verbindungen zwischen Windows 10-Geräten und dem Suchdienst zu sorgen.
4	Besuchen Sie *my*Account, um das Tool für die automatische Proxy-Ermittlung herunterzuladen. Führen Sie die Datei aus, um eine .war-Datei zu extrahieren, und stellen Sie sie im Stamm des Java-Anwendungsservers bereit.
5	Aktualisieren Sie die wdp.properties-Datei der Suchdienst-Webanwendung, um eine Liste der SRP-IDs Ihres Unternehmens hinzuzufügen.

Bereitstellen eines Suchdienstes zur Vereinfachung von Windows 10-Aktivierungen

Die folgenden Schritte zeigen, wie Sie die Suchdienst-Webanwendung in der unten beschriebenen Umgebung bereitstellen können.

Bevor Sie beginnen: Stellen Sie sicher, dass die folgende Software in Ihrer Umgebung installiert ist und ausgeführt wird:

- Windows Server 2012 R2
- Java JRE 1.8 oder höher
- Apache Tomcat 8 Version 8.0 oder höher

1. Konfigurieren Sie eine statische IP-Adresse für den Computer, der den Suchdienst hostet.

Hinweis: Wenn Sie Benutzern die Berechtigung erteilen möchten, Geräte zu aktivieren, wenn sie sich außerhalb des Unternehmensnetzwerks befinden, muss der Zugriff auf die IP-Adresse extern über Port 443 möglich sein.

2. Erstellen Sie einen DNS-Host-A-Datensatz für den Namen **enterpriseenrollment.<*E-Mail-Domäne*>**, der auf die in Schritt 1 konfigurierte statische IP-Adresse verweist.
3. Durchsuchen Sie in dem Verzeichnis, in dem Sie Apache Tomcat installiert haben, die Datei „server.xml“ nach **8080**, und wenden Sie Kommentar-Tags wie im folgenden Beispiel an:

```
<!--
    <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
    -->
```

4. Durchsuchen Sie **server.xml**, und ändern Sie alle Instanzen von **8443** zu **443**.
5. Suchen Sie nach dem Abschnitt **<Connector port= "443"**, entfernen Sie die Kommentar-Tags darüber und darunter, und ändern Sie sie wie im folgenden Beispiel:

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Users\<Kontoname>
\.keystore" />
```

6. Generieren Sie, während Sie mit dem Konto angemeldet sind, das Sie im Beispiel oben angegeben haben, ein Zertifikat, indem Sie die zwei im folgenden Beispiel gezeigten Befehle ausführen. Wenn Sie aufgefordert werden, Ihren Vor- und Nachnamen einzugeben, geben Sie `enterpriseenrollment.<E-Mail-Domäne>` wie unten angezeigt ein:

```
Dateiname>.csr
```

```
changeit
    What is your first and last name?
      [Unknown]:  enterpriseenrollment.example.com
    What is the name of your organizational unit?
      [Unknown]:  IT Department
    What is the name of your organization?
      [Unknown]:  Manufacturing Co.
    What is the name of your City or Locality?
      [Unknown]:  Waterloo
    What is the name of your State or Province?
      [Unknown]:  Ontario
    What is the two-letter country code for this unit?
      [Unknown]:  CA
    Is CN=enterpriseenrollment.example.com, OU=Business Unit, O=Example
 Company, L=Waterloo, ST=Ontario, C=CA correct?
      [no]:  yes

    C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -certreq -alias tomcat
 -keyalg RSA -file <enterpriseenrollment.example.com>.csr
    Enter key password for <enterpriseenrollment.example.com>
            (RETURN if same as keystore password):
```

7. Senden Sie die Anforderung für die Zertifikatssignatur an eine Zertifizierungsstelle. Die Zertifizierungsstelle sendet eine .p7b-Datei zurück. Beim Beispiel oben würde die Zertifizierungsstelle die Datei `enterpriseenrollment.example.com.p7b` zurücksenden.

- Wenn Sie die Anforderung für die Zertifikatssignatur an eine große, externe Zertifizierungsstelle senden, sollten Benutzer keine weiteren Schritte unternehmen müssen, um die Glaubwürdigkeit des Zertifikats bei der Aktivierung nicht zu gefährden.
- Wenn Sie die Anforderung für die Zertifikatssignatur an eine interne Zertifizierungsstelle senden, müssen Sie das Zertifizierungsstellenzertifikat auf dem Gerät installieren, bevor Sie mit der Aktivierung beginnen.

8. Installieren Sie das Zertifikat mithilfe des im folgenden Beispiel gezeigten Befehls:

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -import -trustcacerts -
alias tomcat -file <filename>.p7b
```

9. Beenden Sie Apache Tomcat.
10. Besuchen Sie myAccount, um das Tool für die automatische Proxy-Ermittlung herunterzuladen. Extrahieren Sie den Inhalt der ZIP-Datei, und starten Sie **W10AutoDiscovery-<*Version*>.exe**.
    Die Datei `W10AutoDiscovery-<Version>.war` wird aus der EXE-Datei in das Verzeichnis `C:\BlackBerry` extrahiert.
11. Suchen Sie in dem Verzeichnis, in dem Sie Apache Tomcat installiert haben, nach dem Ordner `\webapps\ROOT`. Wenn dieser bereits vorhanden ist, löschen Sie den Ordner `\ROOT`.
12. Benennen Sie `W10AutoDiscovery-<Version>.war` in `ROOT.war` um. Verschieben Sie die Datei in den Ordner `\webapps` in dem Verzeichnis, in dem Sie Apache Tomcat installiert haben.
13. Starten Sie Apache Tomcat.
    Apache Tomcat stellt die neue Webanwendung bereit und erstellt einen Ordner vom Typ `\webapp\ROOT`.
14. Führen Sie notepad.exe als Administrator aus. Öffnen Sie in dem Verzeichnis, in dem Apache Tomcat installiert wurde, `\webapps\ROOT\WEB-INF\classes\config\wdp.properties`.
15. Fügen Sie die Host-ID für Ihre BlackBerry UEM-Domäne, wie im Beispiel unten gezeigt wird, zur Zeile `wdp.whitelisted.srpid` hinzu. Sie finden die Host-ID für Ihre BlackBerry UEM-Domäne in der BlackBerry UEM-Verwaltungskonsole. Wenn Sie über mehrere BlackBerry UEM-Domänen verfügen, geben Sie die Host-ID für jede Domäne ein. Führen Sie folgende Aktionen aus:
    a) Klicken Sie in der Menüleiste auf **Einstellungen > Lizenzierung > Lizenzierungsübersicht**.
    b) Klicken Sie auf **Lizenzen aktivieren**.
    c) Klicken Sie in der Dropdown-Liste **Lizenz-Aktivierungsmethode** auf **Host-ID**.

```
wdp.whitelisted.srpid=<Host-ID>, <Host-ID>, <Host-ID>
```

16. Starten Sie Apache Tomcat neu.

Integration von UEM mit Azure Active Directory Join

Sie können BlackBerry UEM in Azure Active Directory integrieren, um den Registrierungsprozess für Windows 10-Geräte zu vereinfachen. Nach der Konfiguration können Benutzer ihre Geräte mit UEM unter Zuhilfenahme ihres Azure Active Directory-Benutzernamens und -Kennworts registrieren. Azure Active Directory Join ist auch für die Unterstützung von Windows Autopilot erforderlich, wodurch Windows 10-Geräte während der Windows 10 vorkonfigurierten Einrichtung automatisch mit UEM aktiviert werden können.

Um Azure Active Directory Join mit UEM zu integrieren, gehen Sie wie folgt vor:

Schritt	Beschreibung
1	Verwenden Sie den Wert der Standardvariablen %ClientlessActivationURL% in UEM, um die folgenden URLs zu bestimmen, damit Sie UEM mit Azure Active Directory Join integrieren können. Beispiel: Im Bildschirm mit den Benutzerdetails eines Benutzers, der die standardmäßige Aktivierungs-E-Mail-Vorlage verwendet, können Sie auf **Aktivierungs-E-Mail anzeigen** klicken, um den Wert von %ClientlessActivationURL% im Feld für den Windows 10-Servernamen zu finden. 1. Bestimmen Sie die URL für die MDM-Nutzungsbedingungen. Die URL hat die folgende Struktur: *%ClientlessActivationURL%*/azure/termsofuse Wenn beispielsweise die Variable %ClientlessActivationURL% in `https://enrol.example.net/S123456789/win/mdm` aufgelöst wird, verwenden Sie `https://enrol.example.net/S123456789/win/mdm/azure/termsofuse`. 2. Ermitteln Sie die MDM-Such-URL. Die URL hat die folgende Struktur: *%ClientlessActivationURL%*/azurs/discovery Wenn beispielsweise die Variable %ClientlessActivationURL% in `https://enrol.example.net/S123456789/win/mdm` aufgelöst wird, verwenden Sie `https://enrol.example.net/S123456789/win/mdm/azure/discovery`. 3. Bestimmen Sie den App-ID-URI nur mithilfe des Hostnamens der Standardvariablen %ClientlessActivationURL%. Wenn beispielsweise die Variable %ClientlessActivationURL% in `https://enrol.example.net/S123456789/win/mdm` aufgelöst wird, verwenden Sie `https://enrol.example.net`.
2	UEM mit Azure Active Directory integrieren.

UEM mit Azure Active Directory integrieren

Bevor Sie beginnen: Bestimmen Sie die MDM-Nutzungsbedingungen URL, MDM-Such-URL und die App-ID-URI. Weitere Informationen finden Sie unter Integration von UEM mit Azure Active Directory Join.

1. Melden Sie sich beim Microsoft Azure-Verwaltungsportal unter https://portal.azure.com an.
2. Navigieren Sie zu **Mobilität (MDM und MAM)**.
3. Klicken Sie auf **Anwendung hinzufügen**.
4. Klicken Sie auf **Lokale MDM-Anwendung**. Geben Sie einen Anzeigenamen ein (z. B. `BlackBerry UEM`).
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf die Anwendung, die Sie im vorherigen Schritt hinzugefügt haben, um ihre Einstellungen zu konfigurieren.
7. Geben Sie den Benutzerbereich an, **Einige** oder**Alle**. Wählen Sie ggf. die Gruppen aus.
8. Geben Sie im Feld **MDM-Nutzungsbedingungen URL** die URL an. Weitere Informationen finden Sie in Schritt 1 unter Integration von UEM mit Azure Active Directory Join.
9. Geben Sie im Feld **MDM-Such-URL** die URL an. Weitere Informationen finden Sie in Schritt 1 unter Integration von UEM mit Azure Active Directory Join.
10. Klicken Sie auf **Speichern**.
11. Klicken Sie auf **Einstellung lokale MDM-Anwendung > Eigenschaften**.

12. Geben Sie im Feld **App-ID-URI** die URL an. Weitere Informationen finden Sie in Schritt 1 unter Integration von UEM mit Azure Active Directory Join.
13. Klicken Sie auf **Speichern**.

Konfiguration von Windows Autopilot in Microsoft Azure

Um die Windows Autopilot-Geräteaktivierung zu unterstützen, gehen Sie wie folgt vor:

Schritt	Beschreibung
1	UEM mit Azure Active Directory integrieren.
2	Erstellen eines Windows Autopilot-Bereitstellungsprofils in Azure und weisen sie Benutzergruppen in Azure zu.
3	Importieren von Windows Autopilot-Geräten nach Azure.

Erstellen eines Windows Autopilot-Bereitstellungsprofils in Azure

Sie müssen den entsprechenden Benutzergruppen in Azure ein Windows Autopilot-Bereitstellungsprofil zuweisen, damit Benutzer ihr Gerät mit Windows Autopilot aktivieren können.

1. Melden Sie sich beim Microsoft Azure-Verwaltungsportal unter https://portal.azure.com an.
2. Navigieren Sie zu **Geräteregistrierung > Windows-Registrierung > Windows Autopilot-Bereitstellungsprofile**.
3. Erstellen Sie ein Windows Autopilot-Bereitstellungsprofil.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Konfigurieren Sie die vorkonfigurierte Einrichtung.
6. Weisen Sie den entsprechenden Benutzergruppen das Profil zu.
7. Klicken Sie auf **Speichern**.

Importieren von Windows Autopilot-Geräten nach Azure

Führen Sie diese Schritte durch, um jedes Windows 10-Gerät zu importieren, das mit Windows Autopilot aktiviert werden soll.

1. Schalten Sie das Windows 10-Gerät ein, um das Gerät sofort einzurichten.
2. Stellen Sie eine Verbindung zu einem Wi-Fi-Netzwerk mit Internetverbindung her.
3. Drücken Sie auf der Tastatur **STRG + UMSCHALT + F3** oder **STRG+Fn+UMSCHALT+F3**. Das Gerät wird neu gestartet und wechselt in den Überwachungsmodus.
4. Führen Sie **Windows PowerShell** als Administrator aus.
5. Führen Sie `Save-Script -Name Get-WindowsAutoPilotInfo -Pfad C:\Windows\Temp` aus, um das Windows PowerShell-Skript zu überprüfen.
6. Führen Sie `Install Script -Name Get-WindowsAutoPilotInfo` aus, um das Skript zu installieren.
7. Führen Sie `Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv` aus, um die Geräteinformationen in einer .csv-Datei zu speichern.

8. Gehen Sie folgendermaßen vor, um eine .csv-Datei in Microsoft Azure zu importieren:
   a) Navigieren Sie im Azure-Portal zu **Geräteregistrierung > Windows-Registrierung > Windows AutoPilot-Geräte**.
   b) Klicken Sie auf **Importieren**.
   c) Wählen Sie die .csv-Datei aus.
9. Führen Sie im Dialogfeld **Systemvorbereitungstool** die folgenden Schritte aus:
   a) Wählen Sie im Feld **Systembereinigungsaktion** die Option **Out-of-Box-Experience (OOBE) für System aktivieren** aus, und deaktivieren Sie die Option **Verallgemeinern**.
   b) Wählen Sie im Feld **Optionen für Herunterfahren** die Option **Neustart** aus.

Migrieren von Benutzern, Geräten, Gruppen und anderen Daten aus einem Quellserver

Über die BlackBerry UEM-Verwaltungskonsole können Sie Benutzer, Geräte, Gruppen und andere Daten von den folgenden Quellservern migrieren:

- BlackBerry UEM (lokal)
- Good Control (Standalone)

Hinweis: Wenn Sie Benutzer, Geräte, Gruppen und andere Daten von einem BES10-Quellserver migrieren möchten, müssen Sie auf BlackBerry UEM Version 12.9 migrieren und dann ein Upgrade auf BlackBerry UEM Version 12.11 durchführen. Eine direkte Migration von BES10 auf BlackBerry UEM Version 12.10 und 12.11 wird nicht unterstützt.

Hinweis: Wenn Sie nur Good Control-Benutzer von einem Good Control-Server migrieren möchten, der in BES12 Version 12.5 integriert ist, finden Sie unter support.blackberry.com/community im Artikel 48870 weitere Informationen.

Hinweis: Weitere Informationen zur Migration von BlackBerry Dynamics-Benutzern und -Geräten in Batches mit .csv-Dateien finden Sie unter support.blackberry.com/community im Artikel 49442.

Führen Sie zum Migrieren von Benutzern, Geräten, Gruppen und anderen Daten die folgenden Schritte durch:

Schritt	Aktion
1	Überprüfen Sie die Migrationsvoraussetzungen.
2	Herstellen einer Verbindung zu einem Quellserver.
3	Migrieren Sie optional IT-Richtlinien, Profilen und Gruppen.
4	Bei einer Migration von einem Good Control-Quellserver siehe Komplette Richtlinie und Profilmigration von Good Control zu BlackBerry UEM.
5	Migrieren Sie Benutzer.
6	Migrieren Sie Geräte.

Voraussetzungen: Migrieren von Benutzern, Geräten, Gruppen und anderen Daten aus einem Quellserver

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie mit der Migration beginnen.

Voraussetzung	Details
Anmelden	Melden Sie sich bei BlackBerry UEM als Sicherheitsadministrator an.
Überprüfen der Softwareversion	So migrieren Sie Daten auf BlackBerry UEM: • Die BlackBerry UEM-Instanz, aus der Sie Daten migrieren, muss in Version 12.9 oder höher vorliegen. • Die Good Control (Standalone)-Instanz, aus der Sie Daten migrieren, muss in Version 5.0 oder höher vorliegen.
BlackBerry UEM-Synchronisierung	Ein Good Control-Server darf NICHT in irgendeiner Weise vor Beginn der Migration in BlackBerry UEM integriert werden.
Konfigurieren der Verbindung mit dem BlackBerry UEM-Unternehmensverzeichnis	Konfigurieren Sie die Verbindung mit dem BlackBerry UEM-Zielunternehmensverzeichnis auf die gleiche Weise wie in der Quelle. Wenn die Quelle beispielsweise für die Active Directory-Integration konfiguriert und mit der Domäne „beispiel.com“ verbunden ist, konfigurieren Sie das BlackBerry UEM-Ziel für die Active Directory-Integration und die Verbindung mit der Domäne „beispiel.com“. **Wichtig:** Die Migration funktioniert nicht, wenn das Unternehmensverzeichnis auf dem Zielserver nicht mit dem Unternehmensverzeichnis auf dem Quellserver übereinstimmt.
Defragmentieren der Datenbanken (BlackBerry UEM)	Defragmentieren Sie die Quelldatenbanken und die BlackBerry UEM-Zieldatenbank (sofern vorhanden), bevor Sie die Migration beginnen. Wenn Sie eine große Benutzerzahl migrieren, sollten Sie die BlackBerry UEM-Zieldatenbank nach jeder Migration einer Benutzergruppe defragmentieren. Weitere Informationen zur Defragmentierung einer Microsoft SQL Server-Datenbank finden Sie unter www.technet.microsoft.com im Artikel „Neuorganisieren und Neuerstellen von Indizes“.
Überprüfen des Status der BlackBerry Dynamics-Apps	Prüfen Sie die Version aller BlackBerry Dynamics-Apps, die Sie migrieren möchten. Dies schließt Apps von Erstanbietern, BlackBerry Dynamics-Apps, ISV-Apps von Drittanbietern und interne benutzerdefinierte Apps mit ein. Alle Apps müssen BlackBerry Dynamics SDK Version 4.0.0 oder höher aufweisen. Um zu ermitteln, welche Version von SDK für die zu migrierenden Apps verwendet wird, führen Sie den Containeraktivitätsbericht auf Good Control durch. **BlackBerry Dynamics-Apps, die keine Migration unterstützen, werden vom Gerät gelöscht, wenn der Administrator die Migration startet.**

Voraussetzung	Details
Überprüfen des Status der BlackBerry Dynamics-App-Berechtigungen	Stellen Sie Folgendes sicher: • Die Ziel-BlackBerry UEM hat die gleiche Liste mit BlackBerry Dynamics-App-Berechtigungen wie der Good Control-Quellserver. • Allen migrierten Benutzerkonten wird die gleiche Liste mit BlackBerry Dynamics-App-Berechtigungen auf der Ziel-BlackBerry UEM zugewiesen wie auf dem Good Control-Quellserver. • Der Authentifikator muss auf dem Good Control-Quellserver und dem BlackBerry UEM-Zielserver identisch sein. Sie können den Authentifikator nach der Migration ändern. Fehlende Berechtigungen führen dazu, dass BlackBerry Dynamics-Apps nach der Migration deaktiviert werden.
Überprüfen der Good Control Unternehmens-IDs	Benutzerdefinierte Apps werden nur migriert, wenn die Quell- und Zielserver dieselbe Good Control-Unternehmens-ID aufweisen. Es ist möglich, zwei Unternehmen zusammenzuführen. Weitere Informationen finden Sie unter support.blackberry.com/community im Artikel 47626.

Herstellen einer Verbindung zu einem Quellserver

Sie müssen eine Verbindung zwischen BlackBerry UEM und dem Quellserver herstellen, von dem aus Daten migriert werden. Sie können mehrere Quellen hinzufügen, es kann jedoch immer nur eine aktive Quelle geben.

Hinweis: Stellen Sie sicher, dass das mit den Anmeldeinformationen für die Datenbank verknüpfte Konto, das Sie für die Anmeldung bei der Datenbank verwenden, über Schreibrechte verfügt.

Hinweis: Wenn Sie Ihren BlackBerry UEM-Quellserver seit der letzten Migration aktualisiert haben, sollten Sie die Quellserverkonfiguration neu erstellen, bevor Sie eine weitere Migration durchführen.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Migration > Konfiguration**.
2. Klicken Sie auf +.
3. Wählen Sie in der Dropdown-Liste **Quelltyp** den Typ des Quellservers aus.
4. Je nach Art des Quellservers, den Sie ausgewählt haben, füllen Sie die Felder wie folgt aus:

Typ des Quellservers	Feld	Inhalt
BlackBerry UEM	Anzeigename	Geben Sie einen beschreibenden Namen für den Quellserver ein.
	Datenbankserver	Geben Sie den Namen des Computers ein, der die Quelldatenbank hostet. Verwenden Sie dabei für einen dynamischen Port das Format <Host>\<Instanz> und für einen statischen Port das Format <Host>:<Port>.

Typ des Quellservers	Feld	Inhalt
	Datenbank-Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der für die Verbindung zur Quelldatenbank verwendet werden soll.
	SQL-Benutzername SQL-Kennwort	Wenn Sie die SQL-Authentifizierung gewählt haben, geben Sie in den Feldern „SQL-Benutzername“ und „SQL-Kennwort“ Ihre Anmeldeinformationen für die Verbindung mit der Quelldatenbank ein.
	Datenbankname	Geben Sie den Namen der Quelldatenbank ein.
	UEM-Quellauthentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der für die Anmeldung an der BlackBerry UEM-Quellverwaltungskonsole verwendet wird.
	Benutzername Kennwort	Geben Sie Ihre Anmeldeinformationen für die Quellverwaltungskonsole ein.
	Domäne	Wenn Sie die Microsoft Active Directory-Authentifizierung ausgewählt haben, geben Sie den Namen der Domäne ein, in der sich die Quellverwaltungskonsole befindet.
Good Control (Standalone)	Anzeigename	Geben Sie einen beschreibenden Namen für den Quellserver ein.
	Hostname vom Quell-Good Control (Standalone)	Geben Sie den FQDN der Good Control-Verwaltungskonsole ein.
	Zertifikat vom Quell-Good Control (Standalone)	Laden Sie das Stammzertifikat der Good Control-Zertifizierungsstelle, um SSL-Verbindungen herzustellen. Die Konfigurationsdatei muss das CER-Format aufweisen. Weitere Anweisungen finden Sie unter „Exportieren des selbst-signierten Stammzertifikats für den Good Control-Server“.

Typ des Quellservers	Feld	Inhalt
	Benutzername Kennwort	Geben Sie Ihre Anmeldeinformationen zur Anmeldung beim Verwaltungskonto der Quellverwaltungskonsole ein. **Hinweis:** Diese Anmeldeinformationen müssen einem Good Control-Administrator mit den Zugriffsrechten MANAGE_CONTAINERS und MANAGE_USERS_AND_GROUPS entsprechen. Das Konto kann entweder ein Good Control-Servicekonto oder ein reguläres Administratorkonto sein, vorausgesetzt, das mit dem Konto verbundene Kennwort ermöglicht Zugriff auf die Verwaltungskonsole. Sie können kein Active Directory-Benutzerkonto mit einem Hardwaretoken ohne Kennwort verwenden.
	Domäne	Geben Sie den Namen der Domäne ein, in der sich das Administratorkonto für die Quellverwaltungskonsole befindet. Sie können dieses Feld leer lassen, wenn der Administrator ein lokaler Benutzer ist, der nicht über eine Domäne verfügt.

5. Klicken Sie auf **Speichern**.
6. Klicken Sie zum Testen der Verbindung zwischen der Quelle und dem Ziel auf **Verbindung testen**.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Informationen zur Migration von IT-Richtlinien, Profilen und Gruppen finden Sie unter Bewährte Verfahren im Abschnitt Migrieren von IT-Richtlinien, Profilen und Gruppen aus einem Quellserver.
- Informationen zur Migration von Benutzern finden Sie unter Überlegungen im Abschnitt Migrieren von Benutzern aus einem Quellserver.
- Informationen, die nach der Migration von Benutzern hilfreich sind, finden Sie unter Migrieren von Geräten aus einem Quellserver.

Exportieren des selbst-signierten Stammzertifikats für den Good Control-Server

Führen Sie die folgende Aufgabe aus, wenn das Good Control-Zertifikat nicht durch ein Drittanbieter-Zertifikat ausgetauscht wurde. BlackBerry UEM stuft Zertifikate von Drittanbietern prinzipiell als vertrauenswürdig ein, sodass Sie das Zertifikat nicht vom Good Control-Server exportieren und in BlackBerry UEM importieren müssen.

Hinweis: Die folgende Aufgabe ist nicht Browser-spezifisch. Ausführliche Anleitungen finden Sie in der Dokumentation des verwendeten Browsers.

1. Navigieren Sie in einem Browser zum Anmeldebildschirm einer Ihrer Good Control-Server. Ihnen wird möglicherweise eine Zertifikat-Fehlermeldung angezeigt, weil die Zertifizierungsstelle, die das Zertifikat signiert hat, Good Control war, und der Browser sie nicht als bekannte Zertifizierungsstelle erkennt.
2. Öffnen Sie das Dialogfeld „Zertifikat“ durch Klicken auf das Symbol „Zertifikat“ im URL-Feld.
3. Klicken Sie auf **Zertifikat anzeigen** oder **Zertifikatinformationen**, um das Menü für die **Zertifikatverwaltung** zu öffnen.

4. Klicken Sie auf die Registerkarte **Zertifizierungspfad**.
5. Wählen Sie das Stammzertifikat aus. Das Stammzertifikat ist das erste Element in der Zertifikathierarchie (z. B. GD12345678 CA).
6. Klicken Sie auf **Zertifikat anzeigen**.
7. Klicken Sie auf die Registerkarte **Details**.
8. Klicken Sie auf **In Datei kopieren** oder **Exportieren**.
9. Wählen Sie entweder das Format **DER encoded binary X.509 (.CER)** oder **Base-64 encoded X.509 (.CER)** aus.
10. Geben Sie einen Speicherort und Dateinamen für das Zertifikat an.
11. Klicken Sie auf **Weiter** oder auf **Speichern**.
12. Klicken Sie auf **Fertigstellen**.

Überlegungen: Migrieren von IT-Richtlinien, Profilen und Gruppen aus einem Quellserver

Eine Migration von einer BlackBerry UEM-Quelle kopiert die folgenden Elemente in die Zieldatenbank:

- Ausgewählte IT-Richtlinien
- E-Mail-Profile
- Wi-Fi-Profile
- VPN-Profile
- Proxy-Profile
- BlackBerry Dynamics-Profile
- Profile für Zertifizierungsstellenzertifikate
- Profile für freigegebenes Zertifikat
- SCEP-Profile
- Profile für Benutzeranmelde-informationen
- Einstellungen für die Zertifizierungsstelle
- Alle Richtlinien und Profile, die mit den Richtlinien und Profilen verknüpft sind, die Sie auswählen

Hinweis: Für Gruppen von BlackBerry UEM werden Benutzer, Rollen, Softwarekonfigurationszuordnungen und Attribute von BlackBerry OS nicht migriert.

Eine Migration von einer Good Control (Standalone)-Quelle kopiert die folgenden Elemente in die Zieldatenbank:

- Richtliniensätze
- Verbindungsprofile
- App-Gruppen
- App-Verwendung (für Zertifikate)
- Zertifikate

BlackBerry UEM

Wenn Sie BlackBerry UEM-IT-Richtlinien, -Profile und -Gruppen in eine andere Domäne migrieren, beachten Sie Folgendes:

Objekt	Überlegungen
Kennwörter für IT-Richtlinien	Wenn eine der von Ihnen ausgewählten IT-Quellrichtlinien für Android-Geräte eine Mindestkennwortlänge von weniger als 4 oder eine Höchstlänge von über 16 vorschreibt, können keine BES12- oder BlackBerry UEM-IT-Richtlinien oder -Profile migriert werden. Heben Sie die Auswahl auf, oder aktualisieren Sie die IT-Quellrichtlinie, und starten Sie die Migration neu.
Profilnamen	Nach der Migration müssen Sie sicherstellen, dass alle Profile für SCEP, Benutzeranmeldeinformationen, freigegebene Zertifikate und Zertifizierungsstellenzertifikate eindeutige Namen haben. Wenn zwei Profile des gleichen Typs den gleichen Namen haben, müssen Sie den Namen eines der Profile bearbeiten.
Verzeichnisgruppen	Für die Migration von Verzeichnisgruppen muss für die Quell- und Zieldatenbank jeweils ein Verzeichnis konfiguriert sein. Dieses Verzeichnis muss in der Quell- und Zieldatenbank auf die gleiche Weise konfiguriert sein. Wenn die Verzeichnisse nicht entsprechend eingerichtet sind, werden die Verzeichnisgruppen nicht migriert.
Verschachtelte Gruppen	Wenn die Quell- und Zieldatenbanken BES12- oder BlackBerry UEM-Datenbanken sind, die in BES5 integriert wurden, können verschachtelte Benutzergruppen nicht migriert werden. Wenn Sie versuchen, verschachtelte Gruppen zu migrieren, ist die Migration anderer Gruppen, Profile und PKI-Konfigurationsinformationen möglicherweise nicht möglich.

Good Control (Standalone)

Wenn Sie Sicherheitsrichtliniensätze, Konnektivitätsprofile, App-Gruppen und Zertifikate von Good Control (Standalone) auf BlackBerry UEM migrieren, beachten Sie die folgenden Richtlinien:

Objekt	Überlegungen
Richtliniensätze	Nach der Migration wird jeder Good Control-Richtliniensatz als die folgenden Elemente in BlackBerry UEM angezeigt: • Eine App-Konfiguration für jede App im Richtliniensatz • Eine Sicherheitsrichtlinie • Eine Konformitätsrichtlinie
Verbindungsprofile	Wenn die BlackBerry Dynamics-Verbindungsprofile von Good Control (Standalone) auf BlackBerry UEM migriert werden, werden die Werte von den App-Servern nicht migriert. Die Werte werden unter Verwendung der Standardwerte vom Ziel-UEM-Server aufgefüllt, genau wie bei der manuellen Erstellung eines neuen BlackBerry Dynamics-Verbindungsprofils in UEM. Wenn die BlackBerry Dynamics-Verbindungsprofile von Good Control (Standalone) auf BlackBerry UEM migriert werden, werden einige Werte von der Registerkarte „Infrastruktur“ nicht migriert. Der Administrator muss jedes migrierte Profil manuell bearbeiten und die Werte für das primäre BlackBerry Proxy-Cluster und das sekundäre BlackBerry Proxy-Cluster einrichten.

Objekt	Überlegungen
App-Gruppen	Die Gruppe „Jeder“ wird migriert, ihr sind aber keine Benutzer zugeordnet, und sie ist nicht mit der Gruppe „Alle Benutzer“ im BlackBerry UEM-Ziel verknüpft. Der Administrator muss sie Benutzern bei Bedarf manuell zuweisen.
Apps	Wenn eine App-Berechtigung vom Quellserver nicht auf dem Zielserver existiert, wird die App-Zuweisung nicht migriert. Die App-Gruppe wird migriert.
App-Verwendung (für Zertifikate)	App-Nutzung wird migriert, ausgenommen: • App-Nutzungen, die bereits auf dem Zielserver vorhanden sind • Nicht-BlackBerry Dynamics-Apps • Benutzerdefinierte Apps von einer anderen Good Control-Organisation

Migrieren von IT-Richtlinien, Profilen und Gruppen aus einem Quellserver

IT-Richtlinien, Profile und Gruppen können optional aus einem Quellserver migriert werden.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Wenn mehr als eine Quelle konfiguriert wurde, klicken Sie im linken Fensterbereich auf **Migration > Konfiguration**, und aktivieren Sie dann das Optionsfeld neben dem Namen des Quellservers, aus dem die Daten migriert werden sollen.
3. Klicken Sie auf **Migration** > **IT-Richtlinien, Profile, Gruppen**.
4. Klicken Sie auf **Weiter**.
5. Aktivieren Sie die Kontrollkästchen für die Elemente, die Sie migrieren möchten.

   Der Name des Quellservers ist für jede Richtlinie und jeden Profilnamen angehängt, wenn diese zum Ziel migriert wurden.
6. Klicken Sie auf **Vorschau**, um die von Ihnen ausgewählten Richtlinien und Profile zu prüfen.
7. Klicken Sie auf **Migrieren**.
8. Um die IT-Richtlinien, Profile und Gruppen zu konfigurieren, klicken Sie auf **IT-Richtlinien und -Profile konfigurieren**. Der Bildschirm **Richtlinien und Profile** wird geöffnet.

Wenn Sie fertig sind: Erstellen Sie auf dem Zielserver die Richtlinien und Profile, die nicht migriert werden konnten, und weisen Sie sie den Benutzern vor der Migration von Geräten zu. Für spezifische Informationen zu der Vorgehensweise bei einer Migration von einem Good Control-Source-Server, siehe Komplette Richtlinie und Profilmigration von Good Control zu BlackBerry UEM.

Schließen Sie die Migration der Richtlinie und des Profils von Good Control nach BlackBerry UEM ab

Nachdem Sie die Benutzer, Geräte, Gruppen und andere Daten von Good Control nach BlackBerry UEM migriert haben, müssen Sie die folgenden Aufgaben am Ziel BlackBerry UEM durchführen. Für Informationen zur Position der Good Control-Funktionen in BlackBerry UEM, siehe Good Control-Funktionen in BlackBerry UEM.

Wiederherstellen der Beziehungen zwischen den Apps, Richtlinien und Benutzern:

- Weisen Sie App-Konfigurationen BlackBerry Dynamics-Apps in Gruppen zu.
- Weisen Sie Konnektivitätsprofile Gruppen zu.
- Weisen Sie migrierte BlackBerry Dynamics-Richtlinien und -Konformitätsrichtlinien Benutzern zu.
- Richten Sie Überschreibungsprofile ein (BlackBerry Dynamics-Profile und Konformitätsprofile).

Verschieben Sie JSON-Dateikonfigurationen von Good Control nach BlackBerry UEM.

Schließen Sie die migrierten Konnektivitätsprofile ab:

- Geben Sie die App-Server-Informationen ein.
- Legen Sie die BlackBerry Proxy-Cluster auf der Registerkarte „Infrastruktur“ fest.

Good Control-Funktionen in BlackBerry UEM

In der folgenden Tabelle sind Good Control-Funktionen den Positionen in BlackBerry UEM zugeordnet, an denen Sie vergleichbare Aufgaben ausführen können.

Good Control-Funktion	Position in BlackBerry UEM
Benutzer und Gruppen	Klicken Sie auf **Benutzer**.
Administratoren	Klicken Sie auf **Einstellungen** > **Administratoren**.
Verwalten von BlackBerry Dynamics-Apps und Berechtigungen	**Apps** und klicken Sie auf die App, die Sie verwalten möchten .
Entfernen, Entsperren, Sperren und Verwalten von Protokollen für BlackBerry Dynamics-Apps	1. Klicken Sie in der Menüleiste auf **Benutzer**. 2. Suchen Sie nach einem Benutzerkonto. 3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzerkontos. 4. Wählen Sie die Registerkarte für das Gerät, auf dem die zu verwaltende App installiert ist. 5. Wählen Sie den Befehl im Abschnitt **BlackBerry Dynamics-Apps** neben der App aus, die Sie verwalten möchten.
Generieren von Zugriffsschlüsseln	1. Klicken Sie auf **Benutzer**. 2. Wählen Sie den Benutzer aus, für den Sie einen Zugriffsschlüssel generieren möchten. 3. Klicken Sie auf **Aktivierungskennwort festlegen**. 4. Wählen Sie die Option **Generieren des BlackBerry Dynamics-Zugriffsschlüssels** aus.
Verwalten von Diensten	Klicken Sie auf **Einstellungen** > **BlackBerry Dynamics** > **App-Dienste**.
App-Gruppen	Klicken Sie auf **Gruppen** > **Benutzer**.
Sicherheitsrichtlinien	Klicken Sie auf **Richtlinien und Profile** > **BlackBerry Dynamics**.
Konformitätsrichtlinien	Klicken Sie auf **Richtlinien und Profile** > **Konformität (BlackBerry Dynamics)**.
Bereitstellungsprofile	Klicken Sie auf **Einstellungen** > **Aktivierungsstandards**.

Good Control-Funktion	Position in BlackBerry UEM
App-spezifische Richtlinien	Klicken Sie auf **Apps** und dann auf die BlackBerry Dynamics-App, die Sie verwalten möchten.
App-Server hinzufügen	Klicken Sie auf **Richtlinien und Profile** > **Verbindungen (BlackBerry Dynamics)**.
Verbindungsprofil	Klicken Sie auf **Richtlinien und Profile** > **BlackBerry Dynamics-Verbindungen**.
Geräterichtlinien	Klicken Sie auf **Richtlinien und Profile** > **Richtlinien** > **IT-Richtlinien**
Gerätekonfigurationen	Klicken Sie auf **Richtlinien und Profile** > **Netzwerke und Verbindungen** und wählen Sie die folgenden Profile: • Wi-Fi • VPN • Proxy • E-Mail • Websymbol • Benutzerdefinierte Payload
Apple DEP	Klicken Sie auf **Einstellungen** > **Externe Integration** > **Apple-Programm zur Geräteregistrierung**.
APNS-Verwaltung	Klicken Sie auf **Einstellungen** > **Externe Integration** > **Apple Push Notification**.
Verwalten des Self-Service für Benutzer	Klicken Sie auf **Einstellungen** > **Self-Service**.
Direct Connect-Einstellungen	Klicken Sie auf **Einstellungen** > **BlackBerry Dynamics** > **Direct Connect**.
Servereigenschaften	Klicken Sie auf **Einstellungen** > **BlackBerry Dynamics** > **Eigenschaften**.
Good Proxy-Clusterkonfiguration	Klicken Sie auf **Einstellungen** > **BlackBerry Dynamics** > **Cluster**.
Vertrauenswürdige Stellen	Klicken Sie auf **Richtlinien und Profile** > **Zertifikate** > **Zertifizierungsstellenzertifikat** Klicken Sie auf **Einstellungen** > **Externe Integration** > **Zertifizierungsstelle**
Zertifikatdefinitionen	Klicken Sie auf **Richtlinien und Profile** > **Zertifikate** > **Benutzeranmeldeinformationen** Klicken Sie auf **Einstellungen** > **Externe Integration** > **Zertifizierungsstelle**
Hochgeladene Zertifikate für Benutzer	Klicken Sie auf **Benutzer**>**Alle Benutzer**>**Benutzerdetails**>**Zusammenfassung**>**IT-Richtlinien und -Profile**

Good Control-Funktion	Position in BlackBerry UEM
App-Nutzung	**BlackBerry Dynamics-Apps die Verwendung von Benutzerzertifikaten und Profilen für Benutzeranmeldeinformationen gestatten** auf den entsprechenden Anwendungsseiten mit den Detailinformationen.
Berichte	Klicken Sie auf **Einstellungen** > **BlackBerry Dynamics** > **Berichte**.
Serverjobs	Klicken Sie auf **Einstellungen** > **BlackBerry Dynamics** > **Jobs**.

Überlegungen: Migrieren von Benutzern aus einem Quellserver

Berücksichtigen Sie die folgenden Punkte, wenn Sie Benutzer in ein BlackBerry UEM-Ziel migrieren:

Objekt	Überlegungen
Maximale Anzahl für die Migration	Sie können maximal 1000 Benutzer gleichzeitig aus einer Quelle migrieren. Ist das Ziel eine von BES5 aktualisierte BlackBerry UEM-Datenbank, können Sie maximal 300 Benutzer gleichzeitig migrieren. Wenn Sie mehr als die maximale Anzahl Benutzer für die Migration auswählen, wird nur die maximale Anzahl Benutzer in das BlackBerry UEM-Ziel migriert. Die verbleibenden Benutzer werden ausgelassen. Wiederholen Sie den Migrationsvorgang so häufig wie nötig, um alle Benutzer aus dem Quellserver zu migrieren. **Hinweis:** Wenn BlackBerry UEM das Zeitlimit während der Migration von 1000 Benutzern überschreitet, versuchen Sie die Migration mit weniger Benutzern.
E-Mail-Adresse	• Benutzer benötigen eine E-Mail-Adresse, bevor die Migration erfolgen kann. • Benutzer, die eine im BlackBerry UEM-Ziel bereits vorhandene E-Mail-Adresse verwenden, können nicht migriert werden. Diese Benutzer erscheinen nicht in der Liste der zu migrierenden Benutzer. • Wenn zwei Benutzer in der Quelle die gleiche E-Mail-Adresse haben, wird nur ein Benutzer auf dem Bildschirm „Migrieren von Benutzern“ angezeigt. • Wenn zwei Benutzer in der Quelle die gleiche E-Mail-Adresse aufweisen, können die auf dem Bildschirm „Migrieren von Geräten“ angezeigten Benutzerinformationen entweder von dem einen oder dem anderen Benutzer stammen.
Gerät	• Wenn ein Benutzer in der Quelle sowohl ein BlackBerry 10-Gerät als auch ein iOS- oder Android-Gerät aufweist und für die Geräte die gleiche E-Mail-Adresse mit unterschiedlichen Benutzernamen verwendet wird, werden nicht alle Geräte migriert. • Wenn ein Benutzer ein BlackBerry 10-Gerät sowie ein iOS-, Android-, Windows- oder macOS-Gerät hatte, muss er nach der Migration für BlackBerry UEM Self-Service dieselben Anmeldeinformationen verwenden wie zuvor für BES10 Self-Service, BES12 Self-Service oder BlackBerry UEM Self-Service.

Objekt	Überlegungen
Kennwort	Nach der Migration müssen lokale Benutzer nach dem ersten Anmelden bei BlackBerry UEM Self-Service Ihr Kennwort ändern. Benutzer, die vor der Migration keine Zugriffsberechtigung für BES12 Self-Service oder BlackBerry UEM Self-Service hatten, erhalten nach der Migration nicht automatisch Berechtigung.
Gruppen	Sie können Benutzer ohne Gruppenzuordnung filtern, um diese Benutzergruppe bei einer Migration mit aufzunehmen.
Good Dynamics	Sie können Benutzer migrieren, denen Good Dynamics-Profile zugewiesen sind.

Migrieren von Benutzern aus einem Quellserver

Sie können Benutzer aus dem Quellserver in das BlackBerry UEM-Ziel migrieren. Nach Abschluss der Migration sind die Benutzer sowohl in Quelle als auch in Ziel vorhanden.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Migration > Benutzer**.
2. Wenn die Quelle auf dem Bildschirm **Migrieren von Benutzern** eine Good Control-(Standalone)-Konfiguration ist, klicken Sie auf **Cache aktualisieren**.

   Der Cache benötigt etwa 10 Minuten, um 1000 Benutzer einzupflegen.

   BlackBerry UEM nimmt die Benutzerdaten in den Cache auf, um die Suchfunktionen zu beschleunigen, aber die Benutzerdaten werden direkt von der Quelle migriert. Das Aktualisieren des Cache ist nur für den ersten Satz der Benutzermigration erforderlich. Danach ist es optional.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie die zu migrierenden Benutzer aus.

   Für Good Control-Migrationen werden nur die ersten 20.000 Benutzer angezeigt. Durchsuchen Sie die Benutzernamen oder E-Mail-Adressen, um bestimmte Benutzer zu finden, die sich möglicherweise nicht unter den ersten 20.000 befinden. Wenn Sie auf „Alle auswählen“ klicken, werden nur die Benutzer auf der ersten Seite ausgewählt. Legen Sie die Seitengröße für die Anzahl von Benutzern fest, die Sie auswählen möchten.

   Wenn bei Good Control-Migrationen Änderungen in der Quelle vorgenommen werden, nachdem der Cache aktualisiert wurde, erscheinen diese Änderungen nicht in den angezeigten Cache-Daten. Sie sollten während einer Migration keine Änderungen am Quellserver vornehmen. Falls Sie dies tun, aktualisieren Sie den Cache regelmäßig.
5. Klicken Sie auf **Weiter**.
6. Weisen Sie den ausgewählten Benutzern mindestens eine Gruppe, eine IT-Richtlinie und mindestens ein Profil zu.

   Weitere Informationen finden Sie in der Dokumentation für Administratoren.
7. Klicken Sie auf **Vorschau**.
8. Klicken Sie auf **Migrieren**.

Wenn Sie fertig sind: Migrieren von Geräten aus einem Quellserver.

Überlegungen: Migrieren von Geräten aus einem Quellserver

Berücksichtigen Sie die folgenden Punkte, wenn Sie Geräte in ein BlackBerry UEM-Ziel migrieren:

Objekt	Überlegungen
Bewährtes Verfahren	Es ist ein bewährtes Verfahren, ein Gerät für jede eindeutige Konfiguration zu migrieren (z. B. verschiedene Gruppen, Richtlinien, App-Konfigurationen usw.), um sicherzustellen, dass der Zielserver korrekt eingerichtet ist, bevor die übrigen Geräte migriert werden.
Maximale Anzahl für die Migration	Sie können maximal 2000 Geräte gleichzeitig aus einem Quellserver migrieren.
Ziel-BlackBerry UEM	Überprüfen Sie vor der Migration von Geräten, ob BlackBerry UEM den Gerätetyp und das Betriebssystem unterstützt.
Benutzer	• Die Benutzer müssen in der BlackBerry UEM-Zieldomäne vorhanden sein. • Für Migrationen von BlackBerry UEM können Sie pro Benutzer nicht mehr als fünf Geräte gleichzeitig migrieren.
iOS-Geräte in einer BlackBerry UEM-Quelle	• Auf den iOS-Geräten muss die aktuelle Version von BlackBerry UEM Client installiert sein. • Alle iOS-Geräte müssen vertrauenswürdig sein (nicht vertrauenswürdige iOS-Geräte können nicht migriert werden). • iOS-Geräte, denen das App-Sperrprofil zugewiesen ist, können nicht migriert werden, weil BlackBerry UEM Client nicht für die Migration geöffnet werden kann.
Android-Geräte in einer BlackBerry UEM-Quelle	• Auf den Android-Geräten muss die aktuelle Version von BlackBerry UEM Client installiert sein. • Sie können Android-Geräte, die ein Arbeitsprofil haben, nicht migrieren.
Windows-Geräte	Windows-Geräte können nicht migriert werden.
macOS-Geräte	macOS-Geräte können nicht migriert werden.
MDM-Steuerelemente (BlackBerry UEM)	Geräte, die über „MDM-Steuerelemente“ aktiviert wurden, können vorübergehend nicht auf E-Mails zugreifen, wenn die Migration beginnt. Der E-Mail-Dienst wird wiederhergestellt, wenn die Migration abgeschlossen ist.

Objekt	Überlegungen
Good Control-Geräte (von Standalone Good Control)	**BlackBerry Dynamics-Apps** • Alle BlackBerry Dynamics-Apps, die mit einer Migration kompatibel sind, werden migriert. **BlackBerry Dynamics-Apps, die mit einer Migration nicht kompatibel sind, werden vom Gerät gelöscht, wenn der Administrator die Migration auslöst.** Diese Apps müssen auf der Ziel-BlackBerry UEM reaktiviert werden. • Inkompatible Apps sind Apps, die mit Versionen von BlackBerry Dynamics SDK erstellt wurden, die älter sind als Version 4.0.0. Vor der Migration können Sie den Containeraktivitätsbericht durchführen, um die SDK-Versionen der Apps zu prüfen. • Auf dem Bildschirm „Migrieren von Geräten“ wird in der Spalte „Inkompatible Container“ die Anzahl der BlackBerry Dynamics-Apps für jedes Gerät angezeigt, die nicht migriert werden können, und die Gesamtanzahl der BlackBerry Dynamics-Apps für jedes Gerät. Klicken Sie auf die Zahl, um die BlackBerry Dynamics-Apps anzuzeigen, die mit einer Migration nicht kompatibel sind. • Stellen Sie sicher, dass der Benutzer über Berechtigungen für die App auf der Ziel-BlackBerry UEM verfügt. Wenn die App keine entsprechende Berechtigung hat, erhält der Benutzer nach der Migration eine Nachricht, dass die App blockiert ist. • BlackBerry Dynamics-Apps werden nicht migriert, wenn die Ziel-BlackBerry UEM bereits Apps für diesen Benutzer registriert hat. • BlackBerry Access for Windows 10 und BlackBerry Access for macOS werden bei der Migration nicht unterstützt. Nach Abschluss der Migration müssen Benutzer diese Apps erneut in UEM registrieren. • Benutzerdefinierte Apps werden nur migriert, wenn die Quell- und Zielserver dieselbe Good Control-Unternehmens-ID aufweisen. Es ist möglich, zwei Unternehmen zusammenzuführen. Weitere Informationen finden Sie unter support.blackberry.com/community im Artikel 47626. **Geräteauthentifizierung** • Geräte mit einem Geräteauthentifikator von Good for Enterprise werden nicht migriert. Nach dem Entfernen von Good for Enterprise als Authentifikator müssen Sie den Cache aktualisieren, bevor Sie mit der Migration fortfahren. Dies ist eine bewährte Vorgehensweise, um sicherzustellen, dass dem Benutzer derselbe Authentifikator auf BlackBerry UEM zugewiesen wird wie auf dem Quellserver. • Der Authentifikator muss auf dem Good Control-Quellserver und dem BlackBerry UEM-Zielserver identisch sein. Sie können den Authentifikator nach der Migration ändern.

Objekt	Überlegungen
	Geräteverwaltung • Good Dynamics MDM-Registrierungen werden nicht migriert. Der Benutzer muss die Registrierung von MDM aufheben. Wenn die Ziel-BlackBerry UEM MDM erfordert, muss der Benutzer das alte MDM-Profil manuell löschen und installieren, den BlackBerry UEM Client aktivieren und das Gerät erneut für MDM registrieren. **Betriebssystem** • Geräte mit unbekanntem Betriebssystem werden nicht migriert. **Chat-Sitzungen** • Der BEMS-Quellserver lässt veraltete Connect-Chat-Sitzungen möglicherweise für bis zu 24 Stunden geöffnet, sodass der Benutzer eventuell vorübergehend von zwei Geräten aus beim Chat angemeldet zu sein scheint. • Ungelesene Connect-Chat-Nachrichten werden während der Migration gelöscht. Benutzer sollten sich vor der Migration von Connect abmelden. **Benutzer** • Wenn ein Benutzer über mehrere Geräte mit BlackBerry Dynamics-Apps verfügt, werden alle Geräte automatisch für die Migration ausgewählt. • Sie können keine Geräte für denselben Benutzer von mehreren Good Control-Quellservern migrieren. Sie können Geräte von mehreren Good Control-Quellen migrieren, die Benutzer können jedoch nicht bereits ein BlackBerry Dynamics-Gerät in der Ziel-BlackBerry UEM haben. **Entsperrschlüssel** • Wenn ein Benutzer das Kennwort für eine BlackBerry Dynamics-App vergisst, nachdem die Migration eingeleitet worden ist, aber bevor die Containermigration abgeschlossen wurde, müssen die Zugriffsschlüssel von der Good Control-Quelle bezogen werden. Nachdem die Migration abgeschlossen wurde, muss der Schlüssel von der Ziel-BlackBerry UEM abgerufen werden. **Zugriffsschlüssel** • Nach der Migration können Zugriffsschlüssel nicht mehr auf dem Good Control-Quellserver generiert werden. **Nach der Migration** • Um die Migration auszulösen, müssen Android-Benutzer ihre Geräte neu starten, um einen Kaltstart der BlackBerry Dynamics-Apps zu erzwingen. Manchmal ist ein zweiter Neustart erforderlich. • iOS-Gerätebenutzer müssen nach oben wischen, um die Apps zu schließen. • Um die Migration auszulösen, wird empfohlen, zuerst die App zu öffnen, die als Authentifikator konfiguriert ist. • Nicht alle Apps werden im Launcher angezeigt, bis die Migration abgeschlossen ist. • Nach der Migration werden die App-Symbolanordnungen im Launcher auf die Standardeinstellung zurückgesetzt. • Geräte laden die VIP-Regeln, Lesezeichen und Benutzer-Zertifikate auf den neuen Server hoch.

Objekt	Überlegungen
JSON-Konfigurationen	• Da JSON-Konfigurationen global sind, könnten durch ihre Migration die JSON-Konfigurationen in der Zieldatenbank überschrieben werden. Daher werden JSON-Konfigurationen nicht migriert. Stellen Sie sicher, dass alle erforderlichen JSON-Konfigurationen auf dem Zielserver erneut angewendet werden.

Kurzanleitung für Gerätemigration

Gerätetyp	Aktivierungstyp/Konfiguration	Migration
BlackBerry 10	Beliebige	Unterstützt
Android	• MDM-Steuerelemente • BlackBerry 2FA	Unterstützt
Android	• BlackBerry Dynamics (UEM zu UEM)	Nicht unterstützt
Android-Geräte mit Arbeitsprofil	Beliebige	Nicht unterstützt
Android Samsung KNOX Workspace-Geräte	Beliebige	Unterstützt
iOS	• MDM-Steuerelemente • Geräteregistrierung nur für BlackBerry 2FA • DEP-Geräte, auf denen BlackBerry UEM Client installiert ist	Unterstützt
iOS	• BlackBerry Dynamics (UEM zu UEM) • DEP-Geräte, auf denen BlackBerry UEM Client installiert ist	Nicht unterstützt
Windows	Beliebige	Nicht unterstützt
macOS	Beliebige	Nicht unterstützt

Migrieren von Geräten aus einem Quellserver

Nachdem Sie die Benutzer aus dem Quellserver in das BlackBerry UEM-Ziel migriert haben, können Sie dessen Geräte migrieren. Die Geräte werden vom Quellserver in das BlackBerry UEM-Ziel verschoben und sind nach der Migration in der Quelle nicht mehr vorhanden.

Bevor Sie beginnen:

- Bevor Sie Geräte migrieren, stellen Sie sicher, dass den migrierten Benutzern die richtigen Richtlinien und Berechtigungen zugewiesen sind.
- Für Migrationen von BlackBerry UEM und BES10: Benachrichtigen Sie Benutzer von iOS-Geräten darüber, dass der BlackBerry UEM Client zum Starten der Migration auf BlackBerry UEM geöffnet werden und der BlackBerry UEM Client bis zum Abschluss der Migration geöffnet bleiben muss.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Migration > Geräte**.
2. Wenn die Quelle auf dem Bildschirm **Migrieren von Geräten** eine Good Control-(Standalone)-Konfiguration ist, klicken Sie auf **Cache aktualisieren**.

   Der Cache benötigt etwa 10 Minuten, um 1000 Geräte einzupflegen.

   BlackBerry UEM nimmt die Gerätedaten in den Cache auf, um die Suchfunktionen zu beschleunigen, aber die Gerätedaten werden direkt von der Quelle migriert. Das Aktualisieren des Cache ist nur für den ersten Satz der Gerätemigration erforderlich. Danach ist es optional.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie die zu migrierenden Geräte aus.

   Für Good Control-Migrationen werden nur die ersten 20.000 Geräte angezeigt. Durchsuchen Sie die Benutzernamen oder E-Mail-Adressen, um bestimmte Benutzer zu finden, die sich möglicherweise nicht unter den ersten 20.000 befinden. Wenn Sie auf „Alle auswählen“ klicken, werden nur die Geräte auf der ersten Seite ausgewählt. Legen Sie die Seitengröße für die Anzahl von Geräten fest, die Sie auswählen möchten.

   Hinweis: Ihnen werden möglicherweise weniger Elemente als die Anzahl der Geräte angezeigt, da der Cache nach Benutzer angezeigt wird und einige Benutzer mehr als ein Gerät haben.

   Wenn bei Good Control-Migrationen Änderungen in der Quelle vorgenommen werden, nachdem der Cache aktualisiert wurde, erscheinen diese Änderungen nicht in den angezeigten Cache-Daten. Sie sollten während einer Migration keine Änderungen am Quellserver vornehmen. Falls Sie dies tun, aktualisieren Sie den Cache regelmäßig.
5. Klicken Sie auf **Vorschau**.
6. Klicken Sie auf **Migrieren**.
7. Um den Status der zu migrierenden Geräte anzuzeigen, klicken Sie auf **Migration** > **Status**.

   Um zu bestimmen, welche BlackBerry Dynamics-Apps migriert wurden, führen Sie den Containeraktivitätsbericht auf Good Control durch.

   Stellen Sie sicher, dass die Good Control-Konfiguration ausgeführt wird, bis die Migration aller Authentifikator-Apps des Benutzers abgeschlossen wurde, selbst dann, wenn alle Geräte migriert werden.

Migrieren von DEP-Geräten

Sie können iOS-Geräte, die bei dem Programm für die Geräteregistrierung (DEP) von Apple registriert sind, aus einer BES12- oder BlackBerry UEM-Quelldatenbank in eine andere BlackBerry UEM-Datenbank migrieren.

Migrieren von DEP-Geräten mit installiertem BlackBerry UEM Client

Sie können iOS-Geräte, die bei dem Programm für die Geräteregistrierung (DEP) von Apple registriert sind und über die Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle“ oder „MDM-Steuerelemente“ aktiviert werden, migrieren.

Bevor Sie beginnen: Deaktivieren Sie in den App-Einstellungen für den BlackBerry UEM Client das Kontrollkästchen **Die App vom Gerät entfernen, wenn das Gerät von BlackBerry UEM entfernt wird**.

1. Erstellen Sie im DEP-Portal einen neuen virtuellen MDM-Server.

2. Verbinden Sie die BlackBerry UEM-Zielinstanz mit dem neuen virtuellen MDM-Server. Weitere Informationen finden Sie unter Konfigurieren von BlackBerry UEM für DEP.

   Stellen Sie sicher, dass das DEP-Profil der BlackBerry UEM-Zielinstanz dem der BES12- oder BlackBerry UEM-Quellinstanz entspricht.
3. Verschieben Sie die DEP-Geräte vom virtuellen MDM-Quellserver auf den neuen virtuellen MDM-Server.
4. Migrieren Sie in der BlackBerry UEM-Verwaltungskonsole die DEP-Geräte aus der Quellinstanz zur BlackBerry UEM-Zielinstanz.

Migrieren von DEP-Geräten ohne BlackBerry UEM Client

iOS-Geräte, die bei dem Programm für die Geräteregistrierung (DEP) von Apple registriert sind und auf denen BlackBerry UEM Client nicht installiert ist, werden in der Liste der Geräte aufgeführt, deren Migration nicht unterstützt wird.

1. Erstellen Sie im DEP-Portal einen neuen virtuellen MDM-Server.
2. Verbinden Sie die BlackBerry UEM-Zielinstanz mit dem neuen virtuellen MDM-Server. Weitere Informationen finden Sie unter Konfigurieren von BlackBerry UEM für DEP.

   Stellen Sie sicher, dass die BlackBerry UEM-Zielinstanz das gleiche DEP-Profil hat wie die Quellinstanz.
3. Verschieben Sie die DEP-Geräte vom virtuellen MDM-Quellserver auf den neuen virtuellen MDM-Server.
4. Setzen Sie alle DEP-Geräte auf die Werkseinstellungen zurück.
5. Aktivieren Sie alle DEP-Geräte erneut.

Konfiguration von BlackBerry UEM für die Unterstützung von BlackBerry Dynamics-Apps

Befolgen Sie die Anweisungen in diesem Abschnitt zur Konfiguration der BlackBerry UEM-Einstellungen für BlackBerry Proxy- und BlackBerry Dynamics-Apps.

Verwalten von BlackBerry Proxy-Clustern

Wenn Sie die erste Instanz von BlackBerry Proxy installieren, erstellt BlackBerry UEM ein BlackBerry Proxy-Cluster mit dem Namen „First“. Wenn nur ein Cluster vorhanden ist, werden zusätzliche BlackBerry Proxy-Instanzen diesem Cluster standardmäßig hinzugefügt. Sie können weitere Cluster erstellen und BlackBerry Proxy-Instanzen zwischen allen verfügbaren Clustern verschieben. Wenn mehr als ein BlackBerry Proxy-Cluster verfügbar ist, werden neue Instanzen nicht automatisch zu einem Cluster hinzugefügt. Die neuen Cluster werden stattdessen als nicht zugeordnet betrachtet und müssen einem der verfügbaren Cluster manuell hinzugefügt werden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics**.
2. Klicken Sie auf **Cluster**.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Erstellen Sie ein neues BlackBerry Proxy-Cluster.	**a.** Klicken Sie auf +. **b.** Geben Sie einen Namen für das Cluster ein. **c.** Klicken Sie auf **Speichern**.
Benennen Sie ein BlackBerry Proxy-Cluster um.	**a.** Klicken Sie auf einen Clusternamen. **b.** Ändern Sie den Namen des Clusters. Jedes Cluster muss über einen eindeutigen Namen verfügen. **c.** Klicken Sie auf **Speichern**.
Verschieben Sie eine BlackBerry Proxy-Instanz in ein anderes BlackBerry Proxy-Cluster.	**a.** Klicken Sie in der Spalte **Server** auf den Namen einer BlackBerry Proxy-Instanz. **b.** Wählen Sie in der Dropdown-Liste BlackBerry Proxy**Cluster** das Cluster aus, zu dem die Instanz hinzugefügt werden soll. **c.** Klicken Sie auf **Speichern**.
Löschen Sie ein leeres BlackBerry Proxy-Cluster.	**a.** Klicken Sie auf × für dieses Cluster. **b.** Klicken Sie auf **Entfernen**.
Aktivieren Sie BlackBerry Proxy für die Aktivierung	Wählen Sie die Option **Für Aktivierung aktiviert** für die BlackBerry Proxy-Instanz aus, die Sie zu Aktivierungszwecken verwenden möchten. Es muss mindestens eine Instanz ausgewählt werden.

Konfigurieren von Direct Connect oder eines Web-Proxy für BlackBerry Proxy-Verbindungen

Die BlackBerry Dynamics-Apps auf den Geräten der Benutzer senden standardmäßig Daten an das BlackBerry Dynamics-NOC. Abhängig vom physischen Abstand zwischen den Geräten und dem BlackBerry Dynamics-NOC können bei einigen Verbindungen Netzwerklatenzen auftreten.

Diese Probleme können durch die Aktivierung von BlackBerry Dynamics Direct Connect verringert werden. Direct Connect ermöglicht BlackBerry Dynamics-Apps das Umgehen der Verbindung zum NOC und das Herstellen einer direkten Verbindung zu einer BlackBerry Proxy-Instanz hinter der Firewall Ihres Unternehmens. Wenn Geräte physisch näher an den BlackBerry Proxy-Instanzen in Ihrer Domäne als am BlackBerry Dynamics NOC sind, kann Direct Connect die Netzwerklatenz reduzieren.

Sie können BlackBerry Dynamics-Apps auch so konfigurieren, dass Daten über einen Web-Proxyserver in der DMZ gesendet werden, wenn sie die Verbindung zu einer BlackBerry Proxy-Instanz herstellen.

Bevor Sie beginnen:

- Wenn Sie Verbindungen von BlackBerry Dynamics-Apps über einen Web-Proxyserver weiterleiten möchten, muss der Proxyserver den HTTP Connect-Befehl unterstützen ohne eine Authentifizierung anzufordern. Die interne Firewall Ihres Unternehmens muss Verbindungen über Port 17533 zulassen.
- Wenn Sie für eine BlackBerry Proxy-Instanz keinen Web-Proxyserver definieren, müssen die internen und externen Firewalls Ihres Unternehmens Verbindungen über Port 17533 zulassen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics**.
2. Klicken Sie auf **Direct Connect**.
3. Klicken Sie auf eine BlackBerry Proxy-Instanz.
4. Um Direct Connect zu aktivieren, markieren Sie das Kontrollkästchen **Direct Connect aktivieren**. Überprüfen Sie im Feld **BlackBerry Proxy-Hostname** den Hostnamen auf Richtigkeit.

   Wenn Sie den Hostnamen ändern, erzeugt die BlackBerry Proxy-Instanz ein neues Zertifikat für Clientverbindungen und sendet eine Anfrage zum Signieren des Zertifikats an die BlackBerry Dynamics-Zertifizierungsstelle.
5. Um einen Web-Proxy zu konfigurieren, aktivieren Sie das Kontrollkästchen **Web-Proxy verwenden**. Geben Sie den vollständig qualifizierten Hostnamen und die Portnummer an.
6. Klicken Sie auf **Speichern**.

Konfigurieren von BlackBerry Dynamics-Eigenschaften

Sie können Eigenschaften, die sich speziell auf die Verwendung von BlackBerry Dynamics-Apps in Ihrem Unternehmen beziehen, konfigurieren. Weitere Informationen zu den einzelnen Eigenschaften und zu den Auswirkungen von Änderungen an Standardeinstellungen finden Sie unter Globale Eigenschaften von BlackBerry Dynamics, BlackBerry Dynamics-Eigenschaften und BlackBerry Proxy-Eigenschaften. Informationen zu bewährten Verfahren zur Konfiguration von BlackBerry Proxy-Eigenschaften finden Sie unter support.blackberry.com/community im Artikel 47875.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics**.
2. Führen Sie einen der folgenden Schritte aus:

   - Um die globalen Eigenschaften zu konfigurieren, klicken Sie auf **Globale Eigenschaften**.
   - Um die Eigenschaften für eine bestimmte BlackBerry UEM-Instanz zu konfigurieren, klicken Sie auf **Eigenschaften**. Klicken Sie in der Dropdown-Liste **Servertyp** auf **BlackBerry Control-Server**, und wählen Sie den BlackBerry UEM-Server, den Sie konfigurieren möchten.

- Um die Eigenschaften für eine bestimmte BlackBerry Proxy-Instanz zu konfigurieren, klicken Sie auf **Eigenschaften**. Klicken Sie in der Dropdown-Liste **Servertyp** auf **BlackBerry Proxy-Server**, und wählen Sie den BlackBerry Proxy-Server, den Sie konfigurieren möchten.

3. Konfigurieren Sie die Eigenschaften nach Bedarf.
4. Klicken Sie auf **Speichern**.

Globale Eigenschaften von BlackBerry Dynamics

In den folgenden Tabellen werden die konfigurierbaren globalen Eigenschaften von BlackBerry Dynamics beschrieben.

Die Spalte „Neustart“ gibt an, ob nach dem Ändern der Eigenschaft ein Neustart von BlackBerry UEM erforderlich ist.

Hinweis: Eigenschaften, die in der Verwaltungskonsole angezeigt, aber hier nicht dokumentiert werden, sind veraltet und werden nicht mehr verwendet.

Certificate Management

Eigenschaft	Beschreibung	Standard	Neu starten
Gültigkeitsdauer des Schlüsselspeichers in Sekunden für PKCS12-Zertifikate einzelner Endbenutzer	Die Lebensdauer (Gültigkeit) des Schlüsselspeichers der PKCS 12-Zertifikate, die Gerätebenutzer zum Signieren von E-Mail-Nachrichten und für die Client-Authentifizierung hochladen können, in Sekunden. **Hinweis:** Diese Eigenschaft ist schreibgeschützt. Sie kann nicht geändert werden.	86400	—

Kommunikation

Eigenschaft	Beschreibung	Standard	Neu starten
cntmgmt.internal.port	Der interne Port für den Containerverwaltungsdienst.	Null (Standardwert 17317)	Ja
cntmgmt.max.conns.above.limi	Die maximale Anzahl der Verbindungen, die über das in der Eigenschaft „cntmgmt.max.conns.persec“ definierte Limit hinaus zulässig sind. **Hinweis:** Ändern Sie diese Einstellung nicht ohne Rücksprache mit dem technischen Support von BlackBerry.	3	Ja

Eigenschaft	Beschreibung	Standard	Neu starten
cntmgmt.max.conns.persec	Die maximale Anzahl der Verbindungen für die Containerverwaltung pro Sekunde. **Hinweis:** Ändern Sie diese Einstellung nicht ohne Rücksprache mit dem technischen Support von BlackBerry.	30	Ja
cntmgmt.max.active.sessions	Die maximale Anzahl der aktiven Sitzungen für die Containerverwaltung.	10000	Ja
cntmgmt.max.idle.count	Die maximale Anzahl der für die Containerverwaltung zulässigen Verbindungen ohne Aktivität. **Hinweis:** Ändern Sie diese Einstellung nicht ohne Rücksprache mit dem technischen Support von BlackBerry.	0	Ja
cntmgmt.max.read.throughput	Die maximale Anzahl gleichzeitiger Lesevorgänge für die Containerverwaltung. **Hinweis:** Ändern Sie diese Einstellung nicht ohne Rücksprache mit dem technischen Support von BlackBerry.	500	Ja
cntmgmt.max.write.throughput	Die maximale Anzahl gleichzeitiger Schreibvorgänge für die Containerverwaltung. **Hinweis:** Ändern Sie diese Einstellung nicht ohne Rücksprache mit dem technischen Support von BlackBerry.	500	Ja
cntmgmt.ssl.external.enable	Steuert die SSL-Aktivierung für die externe Containerverwaltung.	Aktiviert	Ja
cntmgmt.ssl.internal.enable	Steuert die SSL-Aktivierung für die interne Containerverwaltung.	Aktiviert	Ja

Doppelte Container

Wenn BlackBerry UEM doppelte Container auf Geräten erkennt, werden Batchaufträge geplant, um diese zu entfernen. Ein doppelter Container weist dieselbe Benutzer-ID und Berechtigungs-ID (auch als BlackBerry Dynamics-App-ID bezeichnet) auf wie ein anderer Container auf demselben Gerät. Wenn ein doppelter Container entfernt wird, wird dieser Vorgang in der BlackBerry UEM-Protokolldatei erfasst.

Eigenschaft	Beschreibung	Standard	Neu starten
Automatically remove older duplicate containers on same device for the user after provisioning.	Legen Sie fest, ob BlackBerry UEM doppelte Container automatisch entfernt, wenn eine neue Version einer App verfügbar ist. Wenn diese Einstellung ausgewählt wird, hat sie Vorrang vor den anderen Eigenschaften doppelter Container.	Aktiviert	Nein
Auftrag für automatisches Entfernen von doppelten Containern aktivieren (ein/aus)	Legen Sie fest, ob BlackBerry UEM Aufträge zum Erkennen und Entfernen doppelter Container von Geräten automatisch plant.	Aktiviert	Nein
Timeout nach Inaktivität in Sekunden vor dem Löschen doppelter Container	Die Zeitspanne in Sekunden, über die ein doppelter Container inaktiv sein muss, bevor von BlackBerry UEM ein Auftrag zum Entfernen des Containers geplant wird.	259200	Nein
Häufigkeit der Ausführung des Auftrags zum Entfernen des Containers in Sekunden	Gibt an, wie häufig (in Sekunden) BlackBerry UEM einen Auftrag zum Erkennen und Entfernen doppelter Container ausführt.	86400	Nein
Maximale Anzahl der in einem einzelnen Auftrag zu entfernenden Container	Die maximale Anzahl der inaktiven Container, die sich über einen einzelnen Auftrag von Geräten entfernen lassen	100	Nein

Eingeschränkte Kerberos-Delegierung

Eigenschaft	Beschreibung	Standard	Neu starten
Explizites UPN verwenden	Geben Sie an, ob BlackBerry Dynamics-Apps bei der Authentifizierung für Dienste, die mit Microsoft Active Directory oder Exchange ActiveSync in Office 365 integriert sind, eine explizite oder implizite UPN verwenden. Das Active Directory Ihres Unternehmens unterstützt je nach Ihrer Umgebung möglicherweise beide oder nur eine der Optionen.	Deaktiviert	Nein
KCD aktivieren (gc.krb5.enabled)	Legen Sie fest, ob BlackBerry UEM die eingeschränkte Kerberos-Delegierung für BlackBerry Dynamics-Apps unterstützt.	Deaktiviert	Ja

Verschiedenes

Eigenschaft	Beschreibung	Standard	Neu starten
config.command.expiry	Gibt die Wartezeit von BlackBerry UEM bis zum erneuten Senden einer nicht bestätigen Nachricht in Sekunden an.	60	Ja
config.command.retry	Gibt an, wie häufig (in Sekunden) BlackBerry UEM den Vorgang zum Erkennen und erneuten Senden nicht bestätigter Nachrichten ausführt. Wenn diese Eigenschaft auf 0 gesetzt wird, führt BlackBerry UEM den Vorgang nicht aus.	900	Ja
gc.entgw.report.userinfo	Legen Sie fest, ob die Anzeigenamen von Benutzern an das BlackBerry Dynamics NOC weitergegeben werden.	Deaktiviert	Nein
policy.compliance.interval	Gibt an, wie häufig (in Minuten) BlackBerry UEM Konformitätsrichtlinien für alle Richtliniendatensätze aus dem BlackBerry Dynamics NOC abruft.	1440	Ja

Inaktive Container löschen

Wenn BlackBerry UEM inaktive Container auf Geräten erkennt, werden Batchaufträge geplant, um diese zu entfernen. BlackBerry UEM stuft einen Container als inaktiv ein, wenn dieser über einen Standardzeitraum von 90 Tagen keine Verbindung zu BlackBerry UEM hergestellt hat. Wenn ein inaktiver Container entfernt wird, wird dieser Vorgang in der BlackBerry UEM-Protokolldatei erfasst.

Eigenschaft	Beschreibung	Standard	Neu starten
Auftrag für automatisches Entfernen von inaktiven Containern aktivieren (ein/aus)	Legen Sie fest, ob BlackBerry UEM Aufträge zum Erkennen und Entfernen inaktiver Container von Geräten automatisch plant.	Deaktiviert	Nein
Intervall für die Container-Inaktivität in Sekunden	Die Zeitspanne in Sekunden, bevor BlackBerry UEM einen Container als inaktiv einstuft.	7776000	Nein
Häufigkeit der Ausführung des Auftrags zum Entfernen von inaktiven Containern in Sekunden	Gibt an, wie häufig (in Sekunden) BlackBerry UEM einen Auftrag zum Erkennen und Entfernen inaktiver Container ausführt.	86400	Nein
Maximale Anzahl der in einem einzelnen Auftrag zu entfernenden Container	Die maximale Anzahl der inaktiven Container, die sich über einen einzelnen Auftrag von Geräten entfernen lassen.	100	Nein

Berichte

Eigenschaft	Beschreibung	Standard	Neu starten
Fester Grenzwert für Datensätze in exportierbaren Berichten, um Speichermangel zu vermeiden	Die maximale Anzahl von Zeilen, die in einen Bericht aufgenommen werden können. Der maximale Wert, der eingegeben werden kann, ist 1000000.	5000	Nein

Richtlinie zur Aufbewahrung von Daten

Eigenschaft	Beschreibung	Standard	Neu starten
Protokoll-Lesevorgänge in der Datenbank	Gibt an, ob BlackBerry Control Lesevorgänge in der BlackBerry Control-Datenbank protokolliert.	Aktiviert	Ja
Serveraufträge löschen	Legen Sie fest, ob Serveraufträge von BlackBerry UEM in regelmäßigen Abständen automatisch gelöscht werden.	Aktiviert	Ja
Intervall zum Löschen von Serveraufträgen (in Tagen)	Wenn „Serveraufträge löschen“ aktiviert ist, legen Sie fest, wie häufig (in Tagen) Serveraufträge von BlackBerry UEM gelöscht werden.	30	Ja

BlackBerry Dynamics-Eigenschaften

Die folgenden Tabellen beschreiben die Eigenschaften, die Sie für die einzelnen BlackBerry UEM Core-Instanzen Ihres Unternehmens konfigurieren können.

Eingeschränkte Kerberos-Delegierung

Eigenschaft	Beschreibung	Standard	Neu starten
Speicherort der Datei „krb5.config“ auf dem GC-Server (gc.krb5.config.file)	Die krb5.conf-Datei wird für die bereichsübergreifende Authentifizierung verwendet, wenn eine vertrauenswürdige CAPATH-Verbindung mit mehreren Kerberos-Domänen vorhanden ist.	Nicht festgelegt	Ja
KCD-Debugging-Modus aktivieren (gc.krb5.debug)	Gibt an, ob BlackBerry UEM Daten auf Fehlerbehebungsebene protokolliert.	Deaktiviert	Ja
Voll qualifizierter Name für das KDC (gc.krb5.kdc)	Der FQDN des Servers, der den Dienst Kerberos Key Distribution Center (KDC) hostet.	Nicht festgelegt	Ja

Eigenschaft	Beschreibung	Standard	Neu starten
Speicherort der Schlüsseltabellendatei (gc.krb5.keytab.file)	Der Speicherort der Kerberos-Schlüsseltabellendatei auf dem Computer, der BlackBerry UEM hostet.	Nicht festgelegt	Ja
Dienstkontoname, unter dem der KDC-Dienst ausgeführt wird (gc.krb5.principal.name)	Der Benutzername des Kerberos-Kontos. Domäne oder Bereich dürfen nicht enthalten sein.	Nicht festgelegt	Ja
Bereich – Active Directory (gc.krb5.realm)	Der Bereich des Kerberos-Kontos.	Nicht festgelegt	Ja

BlackBerry Proxy-Eigenschaften

Die folgenden Tabellen beschreiben die Eigenschaften, die Sie für die einzelnen BlackBerry Proxy-Instanzen Ihres Unternehmens konfigurieren können.

Eigenschaft	Beschreibung	Standard	Neu starten
gp.gps.max.sessions	Maximale Anzahl aktiver Sitzungen. **Hinweis:** Diese Eigenschaft ist schreibgeschützt. Sie kann nicht geändert werden.	15000	—
gp.gps.dns.server.ttl.ms	Zeit, die auf Antwort des DNS-Servers gewartet wird, in Millisekunden. **Hinweis:** Diese Eigenschaft ist schreibgeschützt. Sie kann nicht geändert werden.	1800000	—
gp.gps.server.flowcontrol	Legen Sie fest, ob die Flusskontrolle für den Server aktiviert ist	Deaktiviert	—
gp.gps.tcp.keepalive	Legen Sie fest, ob TCP Keep-alive für den Server aktiviert ist.	Deaktiviert	—
gp.gps.unalias.hostname	Für DNS-Anfragen von App-Servern wird entweder die IP-Adresse oder der Hostname verwendet. Wenn Sie diese Option auswählen, verwendet BlackBerry Proxy inverse DNS-Anfragen mit der IP-Adresse des App-Servers Wenn Sie diese Option nicht auswählen, verwendet BlackBerry Proxy den Hostnamen des App-Servers für DNS-Anfragen	Deaktiviert	Ja

Eigenschaft	Beschreibung	Standard	Neu starten
gp.eacp.command.service.nslo	Ermöglicht LDAP über TCP für Active Directory-Server. Active Directory-Server bieten den LDAP-Dienst über das TCP-Protokoll; so können Clients einen LDAP-Server durch Abfrage der DNS auf einen Eintrag in folgender Form finden: _ldap._tcp.DnsDomainName. Wenn Sie diese Option auswählen, verwendet BlackBerry Proxy LDAP für die DNS-Anfrage eines bestimmten Diensthostnamens. Wenn Sie diese Option nicht auswählen, verwendet BlackBerry Proxy direkte inverse DNS-Anfragen mit dem Diensthostnamen, den Sie angeben.	Deaktiviert	Ja
gc.mdc.hb.timeout	Legen Sie den Heartbeat-Timeout fest.	0	—
gp.proxy.auth.username	Benutzername für die Verbindung mit dem externen Web-Proxyserver	Nicht festgelegt	Nein
gp.proxy.auth.domain	Active Directory-Domäne für die Authentifizierungsanmeldung bei einem externen Web-Proxyserver	Nicht festgelegt	Nein
gp.proxy.auth.password	Kennwort für die Authentifizierung beim externen Web-Proxyserver	Nicht festgelegt	Nein
gp.proxy.https.host	Name des externen Web-Proxyservers	Nicht festgelegt	Nein
gp.proxy.https.port	Portnummer für die HTTPS-Verbindung zum externen Web-Proxyserver	Nicht festgelegt	Nein

Eigenschaft	Beschreibung	Standard	Neu starten
GP Proxy URLs Control	Geben Sie eine der folgenden Optionen ein: 1. NOC-URLs: Wenn diese Option ausgewählt wird, werden nur die Standard-NOC-URLs über den Proxyserver geleitet, der durch die Einstellung „gp.proxy.https.host“ angegeben ist. Anfragen für andere URLs, die über BlackBerry Proxy geleitet werden, sind direkt. 2. Alle weiterleiten: Wenn diese Option ausgewählt wird, werden alle URLs, für die BlackBerry Proxy versucht, eine Verbindung herzustellen, über den Proxyserver weitergeleitet, der durch die Einstellung „gp.proxy.https.host“ angegeben ist. 3. Liste benutzerdefinierter URLs: Wenn diese Option ausgewählt wird, werden nur die URLs, die in der Einstellung „gp.proxy.https.host“ angegeben sind und für die BlackBerry Proxy versucht, eine Verbindung herzustellen, über den Proxyserver weitergeleitet, der durch die Einstellung „gp.proxy.https.host“ angegeben ist.	1	Nein
gp.proxy.urls	Wenn Sie die Option „3“ für „GP Proxy URLs Control“ auswählen, geben Sie die URLs an, die über den Proxy weitergeleitet werden müssen, z. B. URLs für BlackBerry Dynamics-Apps, die mit externen Anwendungsservern kommunizieren müssen und einen HTTP-Proxy benötigen, den der gesamte ausgehende Datenverkehr durchlaufen muss. Weitere Informationen finden Sie unter support.blackberry.com/community im Artikel 42633.	Nicht festgelegt	Ja
gp.proxy.use	Einen externen Web-Proxyserver verwenden	Deaktiviert	Nein

Konfigurieren der Kommunikationseinstellungen für BlackBerry Dynamics-Apps

Sie können die Kommunikationseinstellungen für BlackBerry Dynamics-Apps in der Domäne Ihres Unternehmens konfigurieren. Die Kommunikationseinstellungen ermöglichen Ihnen die sichere Kommunikation in Ihrem Netzwerk mit einem Protokoll Ihrer Wahl. Standardmäßig sind TLSv1, v1.1 und v1.2 zulässig, SSLv3 hingegen nicht. Sie müssen mindestens ein Protokoll auswählen.

Hinweis: Wählen Sie nicht nur SSLv3 aus. Dies kann dazu führen, dass alle Verbindungen zu Clients gelöscht werden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics**.
2. Klicken Sie auf **Kommunikationseinstellungen**.

3. Konfigurieren Sie die Einstellungen nach Bedarf.
4. Klicken Sie auf **Speichern**.

Integrieren von BlackBerry UEM mit Cisco ISE

Cisco Identity Services Engine (ISE) ist eine Software zur Netzwerkverwaltung, die einem Unternehmen die Möglichkeit bietet, den Zugriff von Geräten auf das Unternehmensnetzwerk zu steuern (z. B. Zugriff auf Wi-Fi- oder VPN-Verbindungen zulassen oder verweigern). Cisco ISE-Administratoren können Zugriffsrichtlinien erstellen und durchsetzen, um sicherzustellen, dass nur zugelassene Geräte auf das Unternehmensnetzwerk zugreifen können.

Sie können eine Verbindung zwischen Cisco ISE und BlackBerry UEM herstellen, damit Cisco ISE auf Daten von Geräten zugreifen kann, die auf BlackBerry UEM aktiviert sind. Cisco ISE überprüft Gerätedaten, um festzustellen, ob die Geräte die Zugriffsrichtlinien erfüllen. Beispiel:

- Cisco ISE überprüft, ob das Gerät eines Benutzers auf BlackBerry UEM aktiviert ist. Wenn das Gerät nicht aktiviert ist, kann eine Zugriffsrichtlinie verhindern, dass das Gerät eine Verbindung zu geschäftlichen Wi-Fi- oder zu -VPN-Zugriffspunkten herstellt.
- Cisco ISE überprüft, ob das Gerät eines Benutzers mit BlackBerry UEM richtlinienkonform ist. Wenn das Gerät eine Richtlinie verletzt (z. B. wenn es entsperrt oder gehackt wurde), kann eine Zugriffsrichtlinie verhindern, dass das Gerät eine Verbindung zu Wi-Fi-Zugriffspunkten des Unternehmens oder zu -VPN-Zugriffspunkten herstellt.

Cisco ISE-Administratoren können in der Cisco ISE-Verwaltungskonsole Daten von Geräten anzeigen, sortieren und filtern. Administratoren können außerdem die folgenden Geräteverwaltungsaufgaben durchführen: Sperren eines Geräts, Löschen von Unternehmensdaten von einem Gerät oder Löschen aller Gerätedaten.

führen Sie die folgenden Aktionen aus, um BlackBerry UEM und Cisco ISE zu integrieren:

Schritt	Aktion
1	Stellen Sie sicher, dass die Umgebung Ihres Unternehmens die Anforderungen an die Vernetzung von BlackBerry UEM mit Cisco ISE erfüllt.
2	Erstellen Sie ein BlackBerry UEM-Administratorkonto, das Cisco ISE verwenden kann, um Gerätedaten abzurufen.
3	Fügen Sie das BlackBerry Web Services-Zertifikat zum Cisco ISE-Zertifikatspeicher hinzu.
4	Verbinden Sie BlackBerry UEM mit Cisco ISE, und richten Sie ein Autorisierungsprofil und Zugriffsrichtlinien ein.

Anforderungen: Integration von BlackBerry UEM mit Cisco ISE

Objekt	Anforderungen
Version von Cisco ISE	BlackBerry UEM unterstützt die Integration von Cisco ISE Version 1.2 und höher.

Objekt	Anforderungen
Unterstütztes Betriebssystem	Jedes Betriebssystem, das BlackBerry UEM unterstützt (siehe Kompatibilitätsmatrix), mit Ausnahme der folgenden: • BlackBerry 10 OS Version 10.3.2 oder älter (10.3.3 oder höher erforderlich) • BlackBerry OS (Version 7.1 und älter) • Windows 10 für Desktop
Abhörport	Cisco ISE verwendet den standardmäßigen BlackBerry Web Services-Überwachungsport 18084, um Gerätedaten aus BlackBerry UEM abzurufen. Wenn Port 18084 bei der Installation von BlackBerry UEM nicht verfügbar war, hat die Setupanwendung einen anderen verfügbaren Port für diesen Zweck ausgewählt. Um den richtigen Portwert zu überprüfen, suchen Sie in der BlackBerry UEM Core-Protokolldatei (CORE) nach `(^/ciscoise/.*)`, und notieren Sie sich die vor diesem Text aufgeführte Portnummer.
Firewall	Falls eine Firewall zwischen BlackBerry UEM und Cisco ISE vorhanden ist, konfigurieren Sie die Firewall so, dass HTTPS-Sitzungen zwischen beiden Systemen zulässig sind.

Erstellen Sie ein Administratorkonto, das von Cisco ISE verwendet werden kann.

Cisco Identity Services Engine (ISE) erfordert ein dediziertes BlackBerry UEM-Administratorkonto, das Sie verwenden können, um Informationen über Geräte abzurufen. Sie können ein vorhandenes Administratorkonto verwenden oder ein neues Administratorkonto erzeugen. Es ist ein lokales Administratorkonto (kein Verzeichnisbenutzer) erforderlich. Das Administratorkonto erfordert eine Rolle mit den folgenden Berechtigungen:

- Benutzer und aktivierte Geräte anzeigen
- Geräte verwalten
- Gerät sperren und Nachricht einrichten
- Nur geschäftliche Daten löschen
- Alle Gerätedaten löschen

Standardmäßig verfügen die Rollen „Sicherheitsadministrator“ und „Enterprise-Administrator“ über diese Berechtigungen. Um ein neues Administratorkonto mit einer benutzerdefinierten Rolle zu erstellen, führen Sie die folgenden Schritte über ein Administratorkonto mit der Rolle „Sicherheitsadministrator“ aus.

Bevor Sie beginnen: Wenn Sie eine benutzerdefinierte Rolle für das Administratorkonto erstellen möchten, klicken Sie in der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Administratoren > Rollen >** . Wählen Sie die erforderlichen Berechtigungen aus. Klicken Sie auf **Speichern**.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Benutzer**.
2. Klicken Sie auf **Benutzer hinzufügen**.
3. Klicken Sie auf die Registerkarte **Lokal**.
4. Geben Sie einen Vornamen, Nachnamen, Anzeigenamen, Benutzernamen und eine E-Mail-Adresse an.
5. Geben Sie im Feld **Konsolenkennwort** das Kennwort für das Administratorkonto ein.
6. Aktivieren Sie die Option **Aktivierungskennwort für das Gerät nicht festlegen**.

7. Klicken Sie auf **Speichern**.
8. Klicken Sie in der Menüleiste auf **Einstellungen**.
9. Klicken Sie auf **Administratoren > Benutzer**.
10. Klicken Sie auf .
11. Suchen und klicken Sie auf das Benutzerkonto, das Sie erstellt haben.
12. Klicken Sie in der Dropdown-Liste **Rolle** auf die zuvor erstellte benutzerdefinierte Rolle, die standardmäßige Sicherheitsadministratorrolle oder die standardmäßige Enterprise-Administratorrolle.
13. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Hinzufügen des BlackBerry Web Services-Zertifikats zum Cisco ISE-Zertifikatspeicher

Hinzufügen des BlackBerry Web Services-Zertifikats zum Cisco ISE-Zertifikatspeicher

Um Cisco Identity Services Engine (ISE) für die Verbindung mit BlackBerry UEM zu aktivieren, müssen Sie das BlackBerry Web Services-Zertifikat exportieren und in den Cisco ISE-Zertifikatspeicher importieren. Wenn die BlackBerry UEM-Domain Ihres Unternehmens mehrere Instanzen von BlackBerry UEM aufweist, müssen Sie nur das Zertifikat von einer Instanz exportieren.

Wenn Sie nicht über ein Cisco ISE-Administratorkonto verfügen, senden Sie diese Anweisungen an einen Cisco ISE-Administrator.

Hinweis: Die Schritte ab Schritt 3 beziehen sich auf Cisco ISE Version 1.4. Die neueste Cisco ISE-Dokumentation finden Sie unter Cisco ISE Configuration Guides im *Cisco Identity Services Engine Administrator Guide*.

Bevor Sie beginnen: Erstellen Sie ein Administratorkonto, das von Cisco ISE verwendet werden kann..

1. Navigieren Sie in einem Browser zu **https://<*Servername*>:<*BlackBerry Web Services-Port*>/enterprise/admin/util/ws?wsdl**, wobei *<Servername>* der FQDN des Computers ist, der die BlackBerry UEM Core-Komponente hostet. Der Standardwert für den *<BlackBerry Web Services-Port>* ist 18084.
2. Exportieren Sie das BlackBerry Web Services-Zertifikat, und speichern Sie es auf Ihrem Desktop. Weitere Anleitungen finden Sie in der Dokumentation des verwendeten Browsers.

   Beispiel: Klicken Sie in Google Chrome auf das Schlosssymbol neben der URL. Klicken Sie auf der Registerkarte **Verbindungen** auf **Zertifikatinformationen**. Klicken Sie auf der Registerkarte **Details** auf **Datei kopieren**, und folgen Sie den Anweisungen auf dem Bildschirm.
3. Melden Sie sich bei der Cisco ISE-Verwaltungskonsole an.
4. Klicken Sie in der Menüleiste auf **Administration > System > Zertifikate**.
5. Klicken Sie im linken Fensterbereich auf **Vertrauenswürdige Zertifikate**.
6. Klicken Sie auf **Importieren**. Navigieren Sie zu dem BlackBerry Web Services-Zertifikat, und wählen Sie es aus.
7. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdigkeit für Client-Authentifizierung und Syslog**.
8. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdigkeit für die Authentifizierung von Cisco Services**.
9. Klicken Sie auf **Submit**.

Wenn Sie fertig sind: BlackBerry UEM mit Cisco ISE verbinden.

BlackBerry UEM mit Cisco ISE verbinden

Wenn Sie kein Cisco Identity Services Engine (ISE) Administratorkonto haben, senden Sie diese Anweisungen zusammen mit den erforderlichen Informationen zu Cisco ISE und dem BlackBerry UEM-Administratorkonto an einen BlackBerry UEM-Administrator.

Hinweis: Die folgenden Schritte gelten für Cisco ISE Version 1.4. Die neueste Cisco ISE-Dokumentation finden Sie unter Cisco ISE Configuration Guides im *Cisco Identity Services Engine Administrator Guide*.

Bevor Sie beginnen: Hinzufügen des BlackBerry Web Services-Zertifikats zum Cisco ISE-Zertifikatspeicher.

1. Melden Sie sich bei der Cisco ISE-Verwaltungskonsole an.
2. Klicken Sie in der Menüleiste auf **Verwaltung > Netzwerkressourcen > External MDM**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie im Feld **Name** den Anzeigenamen für die Verbindung ein.
5. Geben Sie im Feld **Hostname oder IP-Adresse** den FQDN oder die IP-Adresse der BlackBerry UEM-Domäne ein.
6. Geben Sie in das Feld **Port** `18084` ein.

   Wenn Port 18084 bei der Installation von BlackBerry UEM nicht verfügbar war, hat die Setupanwendung einen anderen verfügbaren Port für diesen Zweck ausgewählt. Um den richtigen Portwert zu überprüfen, suchen Sie in der BlackBerry UEM Core-Protokolldatei (CORE) nach `(^/ciscoise/.*)`, und notieren Sie sich die vor diesem Text aufgeführte Portnummer.
7. Geben Sie im Feld **Benutzername** den Benutzernamen des BlackBerry UEM-Administratorkontos ein.
8. Geben Sie im Feld **Kennwort** das Kennwort für das BlackBerry UEM Administratorkonto ein.
9. Geben Sie im Feld **Abfrageintervall** ein, wie oft (in Minuten) Cisco ISE Gerätedaten von BlackBerry UEM abrufen soll. Es wird empfohlen, den Standardwert von 240 Minuten zu verwenden.

   Hinweis: Wenn Sie diesen Wert auf 60 Minuten oder weniger setzen, kann sich dies deutlich auf die Leistung Unternehmensumgebung auswirken. Wenn Sie diesen Wert auf 0 setzen, ruft Cisco ISE keine Daten von BlackBerry UEM ab.
10. Klicken Sie auf das Kontrollkästchen **Aktivieren**.
11. Klicken Sie auf **Verbindung testen**, um zu prüfen, ob Cisco ISE eine Verbindung zu BlackBerry UEM herstellen kann.
12. Klicken Sie auf **Submit**.

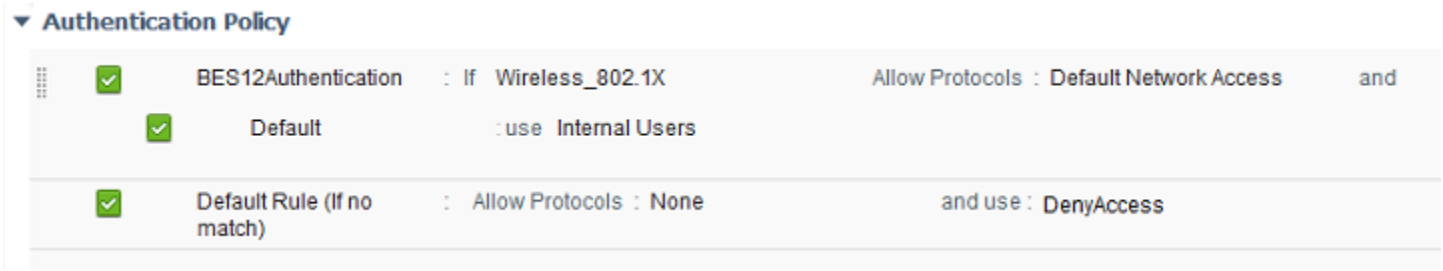
Nachdem die Verbindung hergestellt wurde, können Sie die Wörterbuchattribute für BlackBerry UEM unter **Richtlinie > Richtlinienelemente > Wörterbücher > System > MDM > Wörterbuchattribute** abrufen. Protokolleinträge für die Cisco ISE-Abfrage werden in die BlackBerry UEM Core (CORE)-Protokolldatei geschrieben.

Wenn Sie fertig sind: Führen Sie die folgenden Konfigurationsaufgaben in der Cisco ISE-Verwaltungskonsole aus. Die neuesten Anweisungen finden Sie unter Cisco ISE Configuration Guides im *Cisco Identity Services Engine Administrator Guide* (siehe Set Up MDM Servers With Cisco ISE).

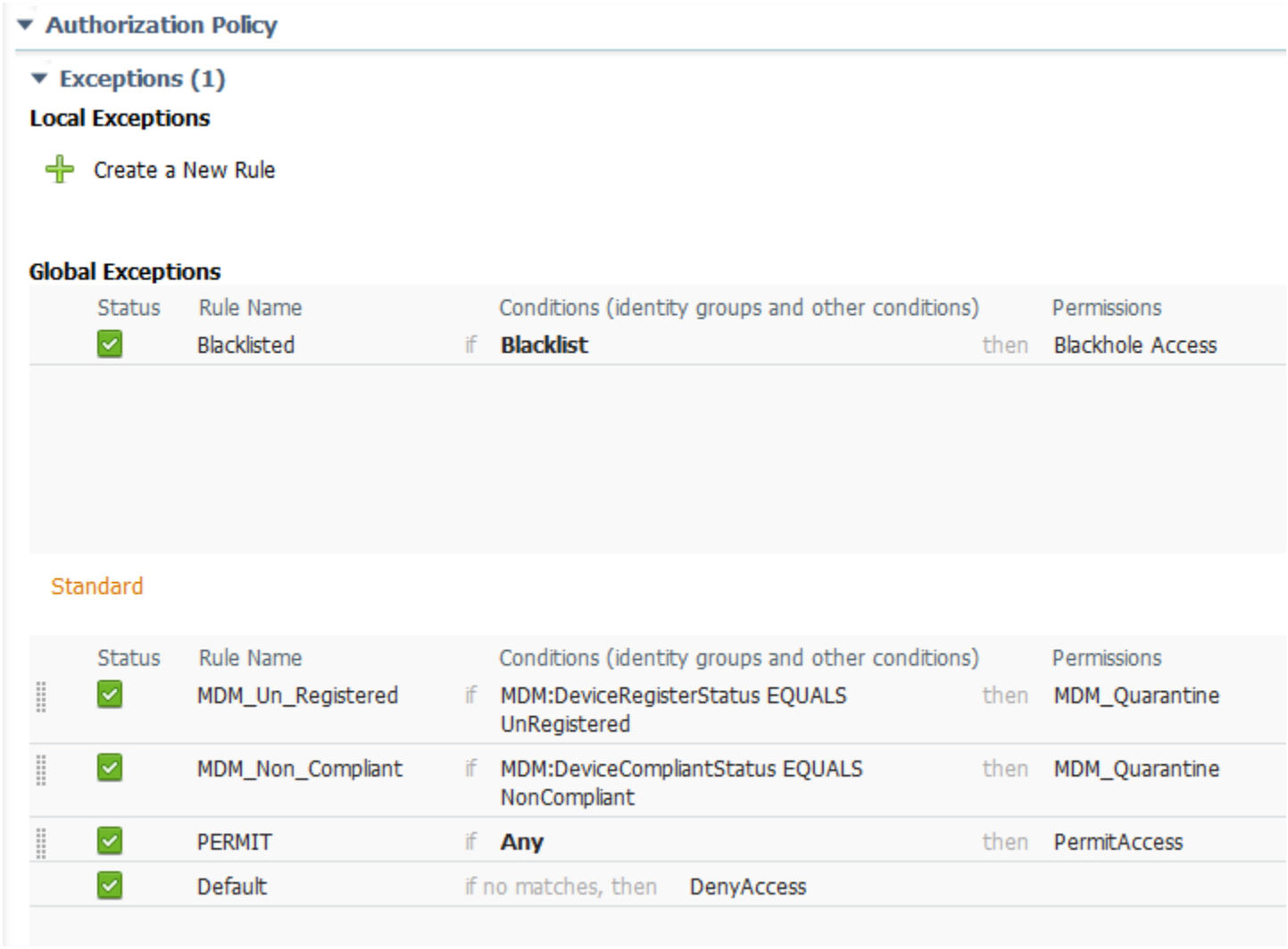
- Konfigurieren Sie ACLs auf dem Wireless-LAN-Controller.
- Konfigurieren Sie ein Berechtigungsprofil für die Umleitung von Geräten, die nicht unter BlackBerry UEM aktiviert wurden. Weitere Informationen finden Sie unter Umleiten von Geräten, die nicht unter BlackBerry UEM aktiviert wurden.
- Konfigurieren Sie Richtlinienregeln für die Autorisierung, die bestimmen, wie Cisco ISE Geräte verarbeitet, die nicht unter BlackBerry UEM aktiviert wurden oder mit BlackBerry UEM nicht richtlinienkonform sind. Erstellen Sie unter **Richtlinie > Richtliniensätze** eine Richtlinie. Ein Beispiel für eine Richtlinie finden Sie unter Beispiel: Authentifizierungsrichtlinienregeln für BlackBerry UEM.

Beispiel: Authentifizierungsrichtlinienregeln für BlackBerry UEM

Authentifizierungsrichtlinie



Autorisierungsrichtlinie



Verwalten von Netzwerkzugriff und Gerätesteuerelementen über Cisco ISE

Cisco Identity Services Engine (ISE)-Administratoren können die folgenden Aktionen durchführen. Weitere Anweisungen finden Sie unter Set Up MDM Servers With Cisco ISE im *Cisco Identity Services Engine Administrator Guide*.

Aktion	Beschreibung
Gerätedaten anzeigen	Sie können Informationen über die mit BlackBerry UEM verknüpften Geräte anzeigen, z. B.: • MAC-Adresse: die eindeutige MAC-Adresse des Geräts • Konformität: ob das Gerät mit BlackBerry UEM richtlinienkonform ist • Festplattenverschlüsselung: ob Gerätedaten verschlüsselt werden • Anmeldung: ob das Gerät unter BlackBerry UEM aktiviert ist • Jailbreak: ob das Gerät gegen eine der Bedingungen für Richtlinientreue (z. B. im Hinblick auf Jailbreak oder Rooting) verstößt • Pin-Sperre: ob das Gerät ein Kennwort verwendet • Hersteller • Modell • Seriennummer • Betriebssystemversion
Konfigurieren von NAC-Richtlinien	Konfigurieren Sie Zugriffsrichtlinien, die steuern, ob Geräte eine Verbindung zu geschäftlichen Wi-Fi- oder VPN-Zugriffpunkten herstellen können. Sie können zum Beispiel eine Zugriffsrichtlinie festlegen, die verhindert, dass Geräte, die nicht mit BlackBerry UEM richtlinienkonform sind, auf das Unternehmensnetzwerk zugreifen.
Gerät sperren	Sperren Sie das iOS-, Android- oder Windows-Gerät eines Benutzers (BlackBerry 10-Geräte unterstützen diese Funktion nicht). Diese Funktion ist nützlich, wenn das Gerät eines Benutzers vorübergehend verlegt wurde. BlackBerry UEM sperrt das Gerät mithilfe eines IT-Administrationsbefehls. Der Benutzer muss das Gerätekennwort eingeben, um das Gerät zu entsperren. Gerätebenutzer können diese Aktion auch über das My Device portal ausführen.
Geschäftliche Daten löschen	Löschen Sie nur geschäftliche Daten und Apps von einem Gerät, sodass die persönlichen Daten und Anwendungen des Benutzers erhalten bleiben. Diese Funktion ist nützlich, wenn das Gerät eines Benutzers verloren gegangen ist oder der Benutzer nicht länger Angestellter des Unternehmens ist. BlackBerry UEM löscht geschäftliche Daten mithilfe eines IT-Administrationsbefehls. Gerätebenutzer können diese Aktion auch über das My Device portal ausführen.

Aktion	Beschreibung
Alle Daten löschen	Löschen Sie alle Daten und Anwendungen von einem Gerät, und setzen Sie das Gerät auf die Werkseinstellungen zurück. Diese Funktion ist nützlich, wenn das Gerät eines Benutzers verloren geht oder gestohlen wird, oder wenn das Gerät an einen anderen Benutzer zugeteilt wird. BlackBerry UEM löscht alle Gerätedaten mithilfe eines IT-Administrationsbefehls. Gerätebenutzer können diese Aktion auch über das My Device portal ausführen.

Weitere Informationen zu IT-Administrationsbefehlen und Aktivierungsarten, die Befehle zum Sperren, Löschen geschäftlicher Daten und Löschen aller Daten unterstützen finden Sie in der Dokumentation für Administratoren.

Umleiten von Geräten, die nicht unter BlackBerry UEM aktiviert wurden

Wenn Cisco Identity Services Engine (ISE) ein Gerät erkennt, das auf das geschäftliche Netzwerk (Wi-Fi oder VPN) zugreifen will, und das Gerät nicht unter BlackBerry UEM aktiviert ist, öffnet Cisco ISE eine Anmeldungsseite im Gerätebrowser, die den Benutzer zur BlackBerry UEM Self-Service-Konsole umleitet.

Der Benutzer benötigt ein BlackBerry UEM-Benutzerkonto für die Anmeldung bei BlackBerry UEM Self-Service und die Aktivierung des Geräts. Teilen Sie den Benutzern mit, dass sie sich an den BlackBerry UEM-Administrator wenden müssen, wenn sie von Cisco ISE auf die Anmeldungsseite umgeleitet werden.

Weitere Informationen zum Hinzufügen und Aktivieren von Administratorkonten finden Sie in der Dokumentation für Administratoren.

Hinweis: Wenn das Gerät eines Benutzers zuvor mit BlackBerry UEM aktiviert war und dann deaktiviert wurde, wird der Benutzer nicht zu BlackBerry UEM Self-Service umgeleitet, falls er versucht, über das Gerät auf das geschäftliche Netzwerk zuzugreifen. Um dieses Problem zu lösen, löschen Sie die Daten für das Gerät aus BlackBerry UEM, wenn Sie ein Gerät aus Cisco ISE entfernen.

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
Großbritannien

Veröffentlicht in Kanada