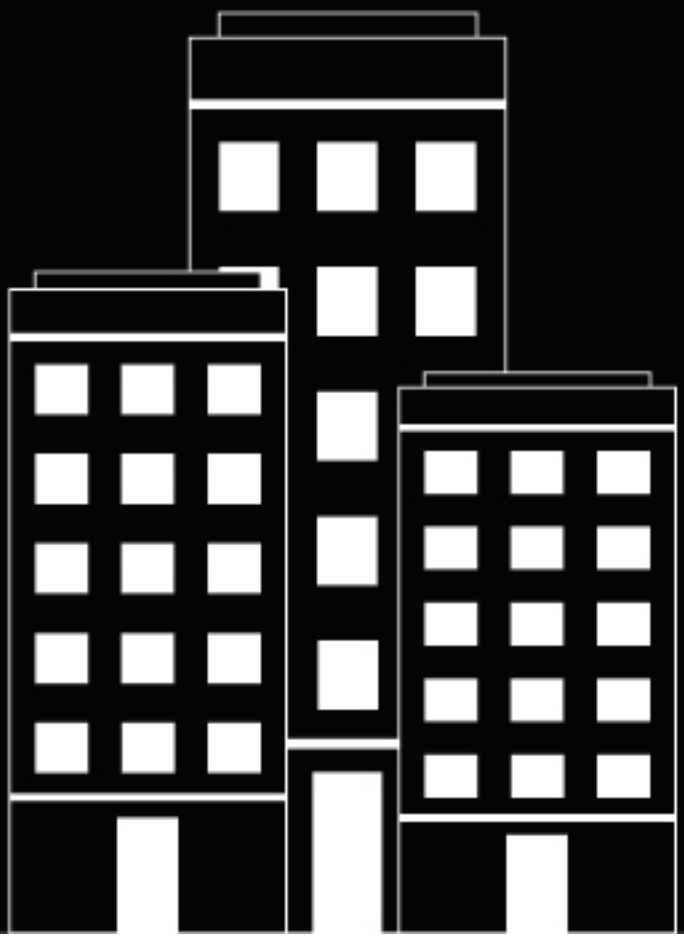

BlackBerry UEM

Konfigurationshandbuch

12.20

Contents

Konfigurieren von BlackBerry UEM

In der folgenden Tabelle sind die ursprünglichen Konfigurationsaufgaben, die in diesem Handbuch besprochen werden, zusammengefasst. Überprüfen Sie sie, um zu bestimmen, welche Aufgaben Sie gemäß den Anforderungen Ihres Unternehmens erledigen sollten. Nach Abschluss der entsprechenden Aufgaben können Sie Administratoren einrichten, Benutzer und Gruppen erstellen und verwalten, Gerätesteuerungen einrichten und Geräte aktivieren.

Wenn Sie die in diesem Handbuch beschriebenen Konfigurationsschritte ausführen, verwenden Sie das bei der Installation von UEM erstellte Administratorkonto. Wenn Sie zusätzliche Administratorkonten für die Konfiguration von UEM erstellen, müssen Sie den Konten die Rolle des Sicherheitsadministrators zuweisen, um sicherzustellen, dass die entsprechenden Berechtigungen erteilt werden.

Aufgabe	Lokal	Cloud	Beschreibung
Ändern der Standardzertifikate, die UEM für die Authentifizierung verwendet	√		Sie können die selbstsignierten Standardzertifikate ersetzen, die von UEM verwendet werden, um die Kommunikation zwischen Komponenten und Geräten zu authentifizieren.
Installieren von BlackBerry Connectivity Node		√	Sie können BlackBerry Connectivity Node in einer UEM Cloud-Umgebung installieren und konfigurieren, um den Zugriff auf das lokale Firmenverzeichnis Ihres Unternehmens zu ermöglichen und Sicherheits- und Konnektivitätsfunktionen zu aktivieren.
Konfigurieren von UEM zum Senden von Daten über einen Proxyserver	√	√	Sie können UEM so konfigurieren, dass Daten zuerst über einen Proxyserver gesendet werden, bevor sie die BlackBerry Infrastructure erreichen. In UEM Cloud-Umgebungen können Sie einen eigenständigen BlackBerry Router als Proxyserver verwenden.
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 UEM-Komponenten mit Remote-Instanzen der Verwaltungskonsole kommunizieren können.
Herstellen einer Verbindung zu einem SMTP-Server zum Senden von E-Mail-Benachrichtigungen	√		Wenn Sie möchten, dass UEM Aktivierungs-E-Mails und andere Benachrichtigungen an Benutzer sendet, müssen Sie die Einstellungen für den SMTP-Server festlegen, den UEM verwenden kann.
Verbinden von UEM mit Unternehmensverzeichnissen	√	√	Verbinden Sie UEM mit Ihren Unternehmensverzeichnissen, um Benutzerkonten zu erstellen, per Verzeichnis verknüpfte Gruppen zu aktivieren und Benutzer-Onboarding und Verzeichnissynchronisierung zu konfigurieren.

Aufgabe	Lokal	Cloud	Beschreibung
Verbinden von BlackBerry UEM mit Entra ID, um Verzeichnisbenutzerkonten zu erstellen	√	√	Verbinden Sie UEM mit Entra, um Verzeichnisbenutzerkonten in UEM zu erstellen.
Konfigurieren von UEM zur Verwaltung von Intune-App-Schutzprofilen	√	√	Verwenden Sie UEM, um Microsoft Intune-App-Schutzprofile zu erstellen, zu verwalten und zuzuweisen, mit denen Daten in Office 365-Apps geschützt werden.
Konfigurieren von UEM als Intune-Konformitätspartner	√	√	Konfigurieren Sie UEM zur Unterstützung des bedingten Zugriffs mit Entra ID.
Registrieren eines APNs-Zertifikats für die Verwaltung von iOS- und macOS-Geräten	√	√	Rufen Sie ein APNs-Zertifikat ab, und registrieren Sie es, wenn Sie Daten verwalten und an iOS- und macOS-Geräte senden möchten.
Konfigurieren von UEM für das Programm zur Geräteregistrierung von Apple	√	√	Mit der UEM-Verwaltungskonsole können Sie iOS-Geräte verwalten, die von Ihrem Unternehmen von Apple für das Programm zur Geräteregistrierung (DEP) erworben wurden.
Konfigurieren von UEM zur Unterstützung von Android Enterprise-Geräten	√	√	Zur Unterstützung von Android Enterprise-Geräten müssen Sie Ihre Google Workspace- bzw. Google Cloud-Domäne zur Unterstützung der Verwaltung mobiler Geräte von Drittanbietern und UEM für die Kommunikation mit Ihrer Google Workspace- bzw. Google Cloud-Domäne konfigurieren.
Konfigurieren von UEM zur Unterstützung von Android Management-Geräten	√	√	Zur Unterstützung von Android Management-Geräten konfigurieren Sie Android Management in der Google Cloud-Konsole und fügen dann eine Android Management-Verbindung in UEM hinzu.
Konfigurieren von UEM für die Verwaltung von Chrome OS-Geräten	√	√	Sie können UEM so konfigurieren, dass bestimmte Chrome OS-Verwaltungsfunktionen unterstützt werden.
Vereinfachen von Windows 10-Aktivierungen	√	√	Sie können diesen Vorgang zur Aktivierung von Windows 10-Geräten vereinfachen, sodass Benutzer keine Serveradresse mehr angeben müssen.
Migrieren von Benutzern, Geräten, Gruppen und anderen Daten aus einem Quellserver	√	√	Sie können Benutzer, Geräte, Gruppen und andere Daten von unterstützten BlackBerry-Servern migrieren.
Konfigurieren der Netzwerkkommunikation und Eigenschaften für BlackBerry Dynamics-Apps	√	√	Sie können die Netzwerkkommunikation und andere Eigenschaften für BlackBerry Dynamics-Apps konfigurieren.

Aufgabe	Lokal	Cloud	Beschreibung
Verschlüsseln der Verbindung zwischen dem BlackBerry UEM und Microsoft SQL Server	√		Sie können die Verbindung zwischen UEM und Microsoft SQL Server verschlüsseln.
Integrieren von UEM in Cisco ISE	√		Sie können eine Verbindung zu Cisco ISE herstellen, damit es Gerätedaten aus UEM abrufen und die Steuerung des Netzwerkzugriffs durchsetzen kann.
Einrichten eines VPN mit Knox StrongSwan für UEM-Dark-Site-Umgebungen	√		In einer UEM-Dark-Site-Umgebung müssen Sie VPN-Zugriff einrichten, damit Samsung Knox-Geräte auf Ihre internen Server und Ressourcen zugreifen können.

Ändern der Zertifikate, die BlackBerry UEM für die Authentifizierung verwendet

Wenn Sie BlackBerry UEM lokal 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 Ihres Unternehmens vorschreiben, dass Zertifikate von der Zertifizierungsstelle Ihres Unternehmens signiert werden, oder wenn Sie Zertifikate verwenden möchten, die von einer Zertifizierungsstelle ausgegeben wurden, denen Geräte und Browser bereits vertrauen.

Wenn beim Ändern eines Zertifikats Probleme auftreten, 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
Apple-Profil-Signaturzertifikat	Das ist ein Zertifikat, das UEM zur Signierung des MDM-Profils verwendet, und 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 Konsolen und BlackBerry Web Services	Das ist ein SSL-Zertifikat, das die Verwaltungskonsole und UEM Self-Service zum Authentifizieren von Browsern verwenden. Wenn Sie eine hohe Verfügbarkeit konfigurieren, muss das Zertifikat den Namen der UEM-Domäne haben. Sie finden den Domänennamen in der Verwaltungskonsole unter Einstellungen > Infrastruktur > Instanzen.
SSL-Zertifikate für BlackBerry Web Services	Das ist ein SSL-Zertifikat, das die BlackBerry Web Services zur Authentifizierung von Anwendungen verwenden, die die BlackBerry Web Services-APIs nutzen, um UEM zu verwalten. Wenn Sie eine hohe Verfügbarkeit konfigurieren, muss das Zertifikat den Namen der UEM-Domäne haben. Sie finden den Domänennamen in der Verwaltungskonsole unter Einstellungen > Infrastruktur > Instanzen.
SSL-Zertifikat für BlackBerry Dynamics-Apps	Das ist ein SSL-Zertifikat, das BlackBerry Dynamics Launcher zum Herstellen eines sicheren Kommunikationskanals mit UEM verwendet. BlackBerry Dynamics-Apps, die die integrierte BlackBerry Dynamics Launcher enthalten, können UEM das Zertifikat für die Authentifizierung beim Server präsentieren.
Zertifikat für Anwendungsverwaltung	Das ist ein SSL-Zertifikat, das für die Authentifizierung zwischen UEM- und BlackBerry Dynamics-Apps verwendet wird. Das Stammzertifizierungsstellenzertifikat wird in der Liste der vertrauenswürdigen Zertifizierungsstellenzertifikate 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 UEM das Zertifikat an alle BlackBerry Dynamics-Apps sendet, müssen alle Apps, die das Zertifikat nicht erhalten haben, erneut aktiviert werden.

Zertifikat	Beschreibung
Zertifikat für Direct Connect	Das ist ein SSL-Zertifikat, das für die Authentifizierung zwischen einem BlackBerry Proxy-Server, der für BlackBerry Dynamics Direct Connect konfiguriert ist, und BlackBerry Dynamics-Apps auf den Geräten verwendet wird. Wenn Sie dieses Zertifikat aktualisieren, wird die neue Version immer über eine Nicht-BlackBerry Dynamics Direct Connect-Verbindung an Geräte gesendet. Alle Geräte oder Container, die zum Zeitpunkt der Änderung nicht online sind, erhalten das Update, wenn sie wieder online gehen. Die Aktualisierung dieses Zertifikats sollte auf dem UEM-Server und allen entsprechenden Network Appliances gleichzeitig durchgeführt werden. Weitere Informationen zum Einrichten von Direct Connect finden Sie unter Konfigurieren von Direct Connect mit BlackBerry UEM.
Zertifikat für BlackBerry Dynamics-Server	Das ist ein SSL-Zertifikat, das Verbindungen zwischen UEM und BlackBerry Proxy authentifiziert.

Überlegungen zum Ändern der BlackBerry Dynamics-Zertifikate

Wenn Sie eines der 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 UEM und BlackBerry Dynamics-Apps gestört werden. Planen und testen Sie Zertifikatänderungen sorgfältig.

Überlegung	Details
Neue Zertifikate zu peripheren Geräten hinzufügen	Wenn Sie BlackBerry Dynamics-Zertifikate zu peripheren Geräten in Ihrem Netzwerk hinzugefügt haben, fügen Sie das neue Zertifikat zu den peripheren Geräten hinzu, bevor Sie es zu UEM hinzufügen.
Verwenden der neuesten Version von BlackBerry Dynamics-Apps	Wenn Sie das BlackBerry Dynamics-Zertifikat für die Anwendungsverwaltung oder Direct Connect ersetzen, stellen Sie sicher, dass Benutzer die aktuellste Version von BlackBerry Dynamics-Apps verwenden, bevor Sie das Zertifikat ersetzen.
BlackBerry Dynamics-Apps müssen geöffnet sein, um ein Zertifikat zu empfangen.	Benutzer müssen BlackBerry Dynamics-Apps auf ihrem Gerät öffnen, damit sie Zertifikate von UEM empfangen kann. Wenn Sie das BlackBerry Dynamics-Zertifikat für Anwendungsverwaltung oder Direct Connect ändern und die Änderung wirksam wird, bevor 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 der BlackBerry Connectivity Node erreichbar ist	Wenn BlackBerry Proxy-Instanzen von UEM nicht erreichbar sind, wenn BlackBerry Dynamics-Zertifikate ersetzt werden, können BlackBerry Dynamics-Apps nach dem Zertifikatersatz keine Verbindung zu diesen Instanzen herstellen.

Überlegung	Details
Zertifikatänderungen 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.

Ändern eines BlackBerry UEM-Zertifikats

Bevor Sie beginnen:

- Lesen Sie Überlegungen zum Ändern der BlackBerry Dynamics-Zertifikate.
- Rufen Sie ein Zertifikat ab, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde. Das Zertifikat muss ein Schlüsselspeicher-Format (.pfx, .pkcs12) aufweisen und mit dem Verschlüsselungstyp TripleDES-SHA1 verschlüsselt werden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Infrastruktur > Serverzertifikate**.
2. Klicken Sie auf den Registerkarten **Serverzertifikate** oder **BlackBerry Dynamics-Zertifikate** im Abschnitt für das Zertifikat, das Sie ersetzen möchten, auf **Details anzeigen**.
3. Klicken Sie auf **Zertifikat ersetzen**.
4. Klicken Sie auf **Durchsuchen**. Navigieren Sie zu der Zertifikatsdatei und wählen Sie sie aus.
5. Geben Sie in das Feld **Verschlüsselungskennwort** oder **Kennwort**ein Kennwort ein.
6. Klicken Sie auf **Ersetzen**.

Wenn Sie fertig sind:

- Wenn Sie eines der Zertifikate auf der Registerkarte Serverzertifikate ersetzt haben, starten Sie den UEM Core-Service auf allen Servern neu.
- Für Zertifikate auf der Registerkarte BlackBerry Dynamics-Zertifikate können Sie auf **Auf Standard zurücksetzen** klicken, um zur Verwendung eines selbstsignierten 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 Sie den selbstsignierten Zertifikaten nicht mehr vertrauen müssen. 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.

Installation von BlackBerry Connectivity Node zur Verbindung mit den Ressourcen hinter der Firewall Ihres Unternehmens

Bei BlackBerry Connectivity Node handelt es sich um eine Sammlung von Komponenten, die Sie auf einem dedizierten Computer installieren können, um weitere Funktionen für BlackBerry UEM Cloud zu aktivieren. Die folgenden Komponenten sind im BlackBerry Connectivity Node enthalten.

Komponente	Zweck
BlackBerry Cloud Connector	Der BlackBerry Cloud Connector ermöglicht UEM Cloud den Zugriff auf das lokale Firmenverzeichnis des Unternehmens. Sie können Verzeichnisbenutzerkonten in UEM erstellen, indem Sie nach Benutzerdaten im Unternehmensverzeichnis suchen und diese importieren. Benutzerdaten werden gemäß dem von Ihnen konfigurierten Zeitplan mit dem Verzeichnis synchronisiert. UEM Cloud muss in der Lage sein, auf Ihr Unternehmensverzeichnis zuzugreifen, wenn Sie SCEP verwenden möchten. Verzeichnisbenutzer können ihre Verzeichnisanmeldeinformationen für den Zugriff auf BlackBerry UEM Self-Service verwenden. Wenn Sie Verzeichnisbenutzern Administratorrollen zuweisen, können die Benutzer sich auch mit ihren Verzeichnisanmeldedaten bei der Verwaltungskonsole anmelden. Der BlackBerry Cloud Connector ermöglicht außerdem das Senden von Zertifikaten an BlackBerry Dynamics-Apps über eine PKI-Verbindung.
BlackBerry Proxy	BlackBerry Proxy hält eine Verbindung zwischen Ihrem Unternehmen und BlackBerry Dynamics NOC aufrecht, die BlackBerry Dynamics-Apps eine sichere Kommunikation mit den Ressourcen Ihres Unternehmens hinter der Firewall ermöglicht. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen von BlackBerry Dynamics NOC ermöglicht. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkkommunikation und Eigenschaften für BlackBerry Dynamics-Apps.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus ermöglicht Benutzern den Zugriff auf geschäftliche Ressourcen hinter der Firewall Ihres Unternehmens, wobei die Sicherheit der Daten mithilfe von Standardprotokollen und durchgehender Verschlüsselung sichergestellt wird. Weitere Informationen finden Sie unter Verwenden von BlackBerry Secure Connect Plus für Verbindungen mit geschäftlichen Ressourcen.
BlackBerry Secure Gateway	BlackBerry Secure Gateway stellt iOS-Geräten mit der Aktivierungsart MDM-Steuerelemente eine sichere Verbindung zum E-Mail-Server Ihres Unternehmens über die BlackBerry Infrastructure zur Verfügung. Weitere Informationen finden Sie unter An iOS-Geräte gesendete E-Mail-Daten mithilfe von BlackBerry Secure Gateway schützen.

Komponente	Zweck
BlackBerry Gatekeeping Service	Der BlackBerry Gatekeeping Service erleichtert die Steuerung der Geräte, die auf Exchange ActiveSync zugreifen können. Weitere Informationen finden Sie unter Steuern, welche Geräte Zugriff auf Exchange ActiveSync haben dürfen.

Die Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node sind in der UEM-Verwaltungskonsole vorhanden. Sie können diese Dateien zur Installation neuer Instanzen des BlackBerry Connectivity Node und für Upgrades vorhandener Instanzen verwenden.

Schritte zum Installieren und Aktivieren von BlackBerry Connectivity Node

Sie können drei oder mehr Instanzen des BlackBerry Connectivity Node installieren, um Redundanz zu bieten.

Schritt	Aktion
1	Überprüfen Sie die Anforderungen und Überlegungen zum Installieren von BlackBerry Connectivity Node.
2	Installieren und Konfigurieren des BlackBerry Connectivity Node.
3	Optional Erstellen einer Servergruppe zur Verwaltung regionaler Verbindungen.
4	Führen Sie eine zusätzliche Konfiguration für BlackBerry Secure Connect Plus, BlackBerry Secure Gateway, den BlackBerry Gatekeeping Service und BlackBerry Dynamics-Apps durch.

Anforderungen: BlackBerry Connectivity Node

Objekt	Anforderungen oder Überlegungen
Hardware	Installieren Sie den BlackBerry Connectivity Node auf einem für technische Zwecke reservierten, dedizierten Computer, d. h. nicht auf einem Computer, der für die tägliche Arbeit genutzt wird. Der Computer muss über Zugriff auf das Internet und Ihr Unternehmensverzeichnis verfügen. Sie können den BlackBerry Connectivity Node nicht auf einem Computer installieren, der bereits eine lokale BlackBerry UEM-Instanz hostet. Sie können drei oder mehr Instanzen des BlackBerry Connectivity Node installieren, um Redundanz zu bieten. Sie müssen jede Instanz auf einem dedizierten Computer installieren. Der Computer, der den BlackBerry Connectivity Node hostet, muss die folgenden Anforderungen erfüllen: • 6 Prozessorkerne, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) oder gleichwertig • 12 GB verfügbarer Arbeitsspeicher • 64 GB Festplattenspeicher
Single-Service-Leistungsmodus	Optional können Sie jedes BlackBerry Connectivity Node-Element in einer Servergruppe so festlegen dass es einen einzelnen Verbindungstyp verarbeitet: nur BlackBerry Secure Connect Plus, nur BlackBerry Secure Gateway oder nur BlackBerry Proxy. Dadurch werden Ressourcen freigegeben, sodass weniger Server für dieselbe Anzahl von Benutzern oder Containern unterstützt werden. Jeder für den Single-Service-Leistungsmodus aktivierte BlackBerry Connectivity Node kann bis zu 10.000 Geräte unterstützen. Wenn Sie den Single-Service-Leistungsmodus für einen BlackBerry Connectivity Node aktivieren, beachten Sie die folgenden Anpassungen der oben aufgeführten Hardwareanforderungen: • Nur BlackBerry Secure Connect Plus: 4 Prozessorkerne, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) oder gleichwertig • Nur BlackBerry Secure Gateway: 8 Prozessorkerne, E5-2670 (2,6 GHz), E5-2683 v4 (2,1 GHz) oder gleichwertig • Nur BlackBerry Proxy: Keine Unterschiede.
Skalierbarkeit und hohe Verfügbarkeit	Jeder BlackBerry Connectivity Node kann bis zu 5000 Geräte unterstützen. Sie können weitere Instanzen installieren, um bis zu 50.000 weitere Geräte zu unterstützen. Sie können mehr als einen BlackBerry Connectivity Node in einer Servergruppe bereitstellen, um eine hohe Verfügbarkeit und Lastverteilung zu erzielen.

Objekt	Anforderungen oder Überlegungen
Software	Der Computer, der die BlackBerry Connectivity Node-Instanz hostet, muss die folgenden Anforderungen erfüllen: • Ein unterstütztes Betriebssystem • Windows PowerShell 2.0 oder höher; erforderlich für die Setup-Anwendung zur Installation von RRAS für BlackBerry Secure Connect Plus und den BlackBerry Gatekeeping Service • Installieren Sie die erforderliche Version von JRE, und legen Sie die Variable BB_JAVA_HOME fest. Weitere Informationen finden Sie unter Einrichtung einer Umgebungsvariable für den Java-Speicherort.
Verzeichnisverbindungen	Stellen Sie sicher, dass Sie einen unterstützten Verzeichnisdienst verwenden. Sie können eine oder mehrere Verzeichnisverbindungen konfigurieren. Wenn Sie jedoch mehrere BlackBerry Connectivity Node-Instanzen haben, müssen alle Verzeichnisverbindungen identisch konfiguriert werden. Wenn eine Verzeichnisverbindung fehlt oder falsch konfiguriert ist, wird dieser BlackBerry Connectivity Node in der Verwaltungskonsole als deaktiviert angezeigt.
Ports	Überprüfen Sie, ob die folgenden ausgehenden Ports in der Firewall Ihres Unternehmens geöffnet sind, sodass die BlackBerry Connectivity Node-Komponenten und ggf. zugeordnete Proxy-Server mit der BlackBerry Infrastructure kommunizieren können: • 443 (HTTPS) zum Aktivieren des BlackBerry Connectivity Node • 3101 (TCP) für alle übrigen ausgehenden Verbindungen
Administratorkonten	Verwenden Sie bei der Installation und Konfiguration des BlackBerry Connectivity Node Administratorkonten, die die folgenden Anforderungen erfüllen: • Verwenden Sie ein Windows-Konto mit Berechtigungen zum Installieren und Konfigurieren der Software auf dem Computer. • Wählen Sie ein Verzeichniskonto mit Leseberechtigungen für jede Verzeichnisverbindung, die Sie konfigurieren möchten. • Verwenden Sie ein UEM Cloud-Administratorkonto mit Berechtigungen zum Herunterladen der BlackBerry Connectivity Node-Installations- und -Aktivierungsdateien (z. B. Sicherheitsadministratorkonto).

Installieren und Konfigurieren des BlackBerry Connectivity Node

Bevor Sie beginnen:

- Überprüfen Sie die Anforderungen und Überlegungen zum Installieren von BlackBerry Connectivity Node.
- Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup**. Klicken Sie auf , und laden Sie die Setupanwendung für den BlackBerry Connectivity Node herunter. Wenn Sie die BlackBerry Connectivity Node-Instanz bei ihrer Aktivierung einer bestehenden Servergruppe zuweisen möchten, klicken Sie in der Dropdown-Liste **Servergruppe** auf die entsprechende Servergruppe. Erstellen und speichern Sie die Aktivierungsdatei. Die Aktivierungsdatei ist 60 Minuten lang gültig.

- Übertragen Sie die Setupanwendung und die Aktivierungsdatei auf den Computer, auf dem die BlackBerry Connectivity Node-Instanz gehostet werden soll. Führen Sie auf diesem Computer die folgenden Schritte aus.

1. Führen Sie die BlackBerry Connectivity Node-Setupanwendung aus.
2. Wählen Sie Ihre Sprache aus. Klicken Sie auf **OK**.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie Ihr Land oder Ihre Region aus. Lesen Sie die Lizenzvereinbarung, und stimmen Sie ihr zu. Klicken Sie auf **Weiter**.
5. Das Installationsprogramm überprüft, ob Ihr Computer die Installationsanforderungen erfüllt. Klicken Sie auf **Weiter**.
6. Klicken Sie zum Ändern des Installationsdateipfads auf **...**, und navigieren Sie zum gewünschten Dateipfad. Klicken Sie auf **Installieren**.
7. Sobald die Installation abgeschlossen ist, klicken Sie auf **Weiter**.

   Die Adresse der BlackBerry Connectivity Node-Konsole wird angezeigt (http:/localhost:8088). Klicken Sie auf den Link, und speichern Sie die Website in Ihrem Browser.
8. Wählen Sie Ihre Sprache aus. Klicken Sie auf **Weiter**.
9. Wenn Sie den BlackBerry Connectivity Node aktivieren, sendet er Daten über Port 443 (HTTPS) an die BlackBerry Infrastructure (z. B. na.bbsecure.com oder eu.bbsecure.com). Nach der Aktivierung verwendet der BlackBerry Connectivity Node Port 3101 (TCP) für alle ausgehenden Verbindungen über die BlackBerry Infrastructure. Wenn Sie Daten vom BlackBerry Connectivity Node über einen vorhandenen Proxy-Server hinter der Firewall des Unternehmens senden möchten, klicken Sie auf **Klicken Sie hier, um die Proxy-Einstellungen der Umgebung Ihres Unternehmens zu konfigurieren**, wählen Sie die Option **Proxy-Server** aus, und führen Sie eine der folgenden Aktionen aus:
   - Um Aktivierungsdaten über einen Proxy-Server zu senden, geben Sie in die Felder **Anmeldungs-Proxy** den FQDN oder die IP-Adresse und die Portnummer des Proxy-Servers ein. Der Proxy-Server muss Daten über Port 443 an bbsecure.com senden können. Klicken Sie auf **Speichern**.
   - Um andere ausgehende Verbindungen von den Komponenten des BlackBerry Connectivity Node über einen Proxy-Server zu senden, geben Sie in die entsprechenden Felder den FQDN oder die IP-Adresse und die Portnummer des Proxy-Servers ein. Der Proxy-Server muss Daten über Port 3101 an bbsecure.com senden können. Klicken Sie auf **Speichern**.
10. Geben Sie im Feld **Anzeigename** einen Namen für den BlackBerry Connectivity Node ein. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Durchsuchen**. Wählen Sie die Aktivierungsdatei aus.
12. Klicken Sie auf **Aktivieren**.

    Wenn Sie eine BlackBerry Connectivity Node-Instanz bei der Aktivierung zu einer bestehenden Servergruppe hinzufügen möchten, muss die Firewall Ihres Unternehmens Verbindungen von diesem Server über Port 443 über die BlackBerry Infrastructure zur Aktivierung des BlackBerry Connectivity Node und zur selben bbsecure.com-Region wie die Hauptinstanz von BlackBerry Connectivity Node zulassen.
13. Klicken Sie auf +, und wählen Sie den Typ des zu konfigurierenden Unternehmensverzeichnisses aus.
14. Folgen Sie den Schritten für den Verzeichnistyp Ihres Unternehmens:

Verzeichnistyp	Schritte
Microsoft Active Directory	**a.** Geben Sie im Feld **Verbindungsname** einen Namen für die Verzeichnisverbindung ein. Wenn Sie ein Microsoft Entra ID-Verzeichnis konfiguriert haben, muss dieser Verbindungsname sich vom Namen der Entra-Verzeichnisverbindung unterscheiden. **b.** Geben Sie im Feld **Benutzername** den Benutzernamen des Microsoft Active Directory-Kontos ein. **c.** Geben Sie im Feld **Domäne** den FQDN der Domäne ein, die Microsoft Active Directory hostet. Beispiel: domain.example.com. **d.** Geben Sie im Feld **Kennwort** das Kennwort für das Microsoft Active Directory-Konto ein. **e.** Klicken Sie in der Dropdown-Liste **Erkennung des Domain Controllers** auf eine der folgenden Optionen: • Wenn Sie die automatische Erkennung nutzen möchten, klicken Sie auf **Automatisch**. • Wenn Sie den Domain Controller-Computer angeben möchten, klicken Sie auf **Aus der Liste unten auswählen**. Klicken Sie auf +, und geben sie den FQDN des Computers ein. Wiederholen Sie diesen Schritt, um weitere Computer hinzuzufügen. **f.** Geben Sie im Feld **Suchbasis des globalen Katalogs** die Suchbasis ein, auf die Sie zugreifen möchten (beispielsweise: OU=Users,DC=example,DC=com). Lassen Sie das Feld leer, um den gesamten globalen Katalog zu durchsuchen. **g.** Klicken Sie in der Dropdown-Liste **Erkennung des globalen Katalogs** auf eine der folgenden Optionen: • Wenn Sie eine automatische Erkennung des Katalogs durchführen möchten, klicken Sie auf **Automatisch**. • Wenn Sie den Katalogcomputer angeben möchten, klicken Sie auf **Aus der Liste unten auswählen**. Klicken Sie auf +, und geben sie den FQDN des Computers ein. Wiederholen Sie diesen Schritt ggf., um weitere Computer anzugeben. **h.** 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 UEM Cloud zugreifen soll, klicken Sie im Abschnitt **Auflisten von Kontengesamtstrukturen** auf +. Geben Sie den Namen der Gesamtstruktur, den Namen der Benutzerdomäne (der Benutzer kann einer beliebigen Domäne in der Kontengesamtstruktur angehören) sowie den Benutzernamen und das Kennwort an. **i.** 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. **j.** Klicken Sie auf **Speichern**.

Verzeichnistyp	Schritte
LDAP-Verzeichnis	**a.** Geben Sie im Feld **Verbindungsname** einen Namen für die Verzeichnisverbindung ein. Wenn Sie ein Microsoft Entra ID-Verzeichnis konfiguriert haben, muss dieser Verbindungsname sich vom Namen der Entra-Verzeichnisverbindung unterscheiden. **b.** Klicken Sie in der Dropdown-Liste **LDAP-Servererkennung** auf eine der folgenden Optionen: • Wenn Sie die automatische Erkennung nutzen möchten, klicken Sie auf **Automatisch**. Geben Sie im Feld **DNS-Domänenname** den DNS-Domänennamen ein. • Wenn Sie den LDAP-Computer angeben möchten, klicken Sie auf **Server aus der Liste unten auswählen**. Klicken Sie auf +, und geben sie den FQDN des Computers ein. Wiederholen Sie diesen Schritt, um weitere Computer hinzuzufügen. **c.** Wählen Sie in der Dropdown-Liste **SSL aktivieren** aus, ob Sie die SSL-Authentifizierung für den LDAP-Verkehr aktivieren möchten. Wenn Sie **Ja** auswählen, klicken Sie auf **Durchsuchen**, und wählen Sie das SSL-Zertifikat für den LDAP-Computer aus. **d.** Geben Sie im Portfeld **LDAP** die Portnummer des LDAP-Computers ein. **e.** Wählen Sie in der Drop-down-Liste **Autorisierung erforderlich** aus, ob UEM Cloud eine Authentifizierung mit dem LDAP-Computer durchführen muss. Wenn Sie **Ja** auswählen, geben Sie den Benutzernamen und das Kennwort des LDAP-Kontos ein. Der Benutzername muss im DN-Format angegeben werden (beispielsweise: CN=Megan Ball,OU=Sales,DC=example,DC=com). **f.** Geben Sie im Feld **Basissuche** die Basissuche ein, auf die Sie zugreifen möchten (beispielsweise: OU=Users,DC=example,DC=com). **g.** Geben Sie im Feld **LDAP-Suchfilter nach Benutzer** den Filter ein, den Sie für LDAP-Benutzer verwenden möchten. Beispielsweise: (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)). **h.** Klicken Sie in der Dropdown-Liste **LDAP-Benutzersuchbereich** auf eine der folgenden Optionen: • Wenn Sie möchten, dass in der Benutzersuche alle Ebenen unter dem Basis-DN durchsucht werden, klicken Sie auf **Alle Ebenen**. • Wenn Sie die Benutzersuche auf eine Ebene unter dem Basis-DN beschränken möchten, klicken Sie auf **Eine Ebene**. **i.** Geben Sie im Feld **Eindeutige Kennung** das Attribut für die eindeutige Kennung der einzelnen Benutzer ein (beispielsweise: uid). Das Attribut muss für jeden Benutzer unveränderbar und global eindeutig sein. **j.** Geben Sie im Feld **Vorname** das Attribut für den Vornamen der einzelnen Benutzer ein (beispielsweise: givenName). **k.** Geben Sie im Feld **Nachname** das Attribut für den Nachnamen der einzelnen Benutzer ein (beispielsweise: sn). **l.** Geben Sie im Feld **Anmeldeattribute** das Anmeldeattribut der einzelnen Benutzer ein (beispielsweise: cn). Dieses Attribut wird für den Wert verwendet, den Benutzer bei der Anmeldung bei BlackBerry UEM Self-Service mit ihren Verzeichnisanmeldeinformationen eingeben. **m.** Geben Sie im Feld **E-Mail-Adresse** das Attribut für die E-Mail der einzelnen Benutzer ein (beispielsweise: mail). **n.** Geben Sie im Feld **Anzeigename** das Attribut für den Anzeigenamen der einzelnen Benutzer ein (beispielsweise displayName). **o.** 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. **p.** Wenn per Verzeichnis verknüpfte Gruppen aktiviert werden sollen, aktivieren

15. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup**.
16. Klicken Sie im Abschnitt **Schritt 4: Verbindung testen** auf **Weiter**.

Um den Status einer BlackBerry Connectivity Node-Instanz anzuzeigen, klicken Sie in der Menüleiste der -Verwaltungskonsole auf **Einstellungen > Externe Integration > Status von BlackBerry Connectivity Node**.

Wenn Sie fertig sind:

- Um weitere BlackBerry Connectivity Node-Instanzen zu installieren, laden Sie die Installations- und Aktivierungsdateien erneut herunter, und wiederholen Sie diese Aufgabe auf einem anderen Computer. Dies sollte durchgeführt werden, nachdem die erste Instanz aktiviert wurde.
- Wenn Sie mehr als einen BlackBerry Connectivity Node installieren, müssen Sie auf jeder Instanz identische Verzeichnisverbindungen konfigurieren. Mit der BlackBerry Connectivity Node-Konsole können Sie die Verzeichnisverbindungen für eine Instanz exportieren (.txt-Datei) und diese Verbindungen dann über die Konsole für diese Instanz zu einem anderen BlackBerry Connectivity Node übertragen und importieren. Entfernen Sie alle vorhandenen Verzeichnisverbindungen aus einer Instanz, bevor Sie Verzeichniskonfigurationen importieren.
- Optional Erstellen einer Servergruppe zur Verwaltung regionaler Verbindungen.
- Wenn Sie Daten über einen HTTP-Proxy senden möchten, bevor diese BlackBerry Dynamics NOC erreichen, klicken Sie in der BlackBerry Connectivity Node-Konsole auf **Allgemeine Einstellungen > BlackBerry Router und Proxy**. Wählen Sie das Kontrollkästchen **HTTP-Proxy aktivieren** aus, und konfigurieren Sie die Proxyeinstellungen.
- Um die Standardeinstellungen von BlackBerry Connectivity Node-Instanzen zu ändern, klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup** und dann auf . Sie können die Protokollierungseinstellungen ändern, Instanzen des BlackBerry Gatekeeping Service deaktivieren und die BlackBerry Secure Gateway-Einstellungen konfigurieren.
- Wenn Sie über eine Aktualisierung von BlackBerry Connectivity Node benachrichtigt werden, wiederholen Sie diese Aufgabe, um die einzelnen Instanzen zu aktualisieren. Mit der BlackBerry Connectivity Node-Konsole können Sie die Verzeichniskonfigurationen aufzeichnen oder exportieren. Sie müssen alle Instanzen von BlackBerry Connectivity Node auf dieselbe Version aktualisieren. Nach dem Upgrade der ersten Instanz werden die Verzeichnisdienste deaktiviert, bis alle Knoten auf dieselbe Version aktualisiert worden sind.
- Anweisungen zum Aktivieren von BlackBerry Secure Connect Plus finden Sie unter Verwenden von BlackBerry Secure Connect Plus für Verbindungen mit geschäftlichen Ressourcen in der Dokumentation für Administratoren.
- Weitere Informationen zum Aktivieren von BlackBerry Secure Gateway finden Sie unter An iOS-Geräte gesendete E-Mail-Daten mithilfe von BlackBerry Secure Gateway schützen in der Dokumentation für Administratoren.
- Anleitungen zum Konfigurieren von BlackBerry Gatekeeping Service finden unter Steuern, welche Geräte Zugriff auf Exchange ActiveSync haben dürfen in der Dokumentation für Administratoren.

Erstellen einer Servergruppe zur Verwaltung regionaler Verbindungen

Wenn Sie regionale Verbindungen für die von BlackBerry Connectivity Node angebotenen Enterprise-Konnektivitätsfunktionen verwalten möchten, können Sie mehrere Instanzen von BlackBerry Connectivity Node in einer dedizierten Region als Servergruppe bereitstellen. Beim Erstellen einer Servergruppe geben Sie den regionalen Datenpfad an, den die zu verwendenden Komponenten für die Verbindung mit der BlackBerry Infrastructure nutzen sollen. Servergruppen unterstützen außerdem Redundanz, Hochverfügbarkeit und Lastausgleich für BlackBerry Connectivity Node-Instanzen.

Bevor Sie beginnen: Installieren und Konfigurieren mehrerer Instanzen von BlackBerry Connectivity Node.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup**.
2. Klicken Sie auf .
3. Geben Sie einen Namen und eine Beschreibung für die Servergruppe ein.
4. Klicken Sie in der Dropdown-Liste **Land** auf das entsprechende Land.
5. Wenn Sie die Unternehmensverzeichnis-Verbindung für die Instanzen in der Servergruppe deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Einstellungen für Verzeichnisdienst überschreiben**.
6. Standardmäßig ist der BlackBerry Gatekeeping Service in jeder BlackBerry Connectivity Node-Instanz aktiv. Wenn die Gatekeeping-Daten nur von der BlackBerry Connectivity Node-Hauptinstanz verwaltet werden sollen, aktivieren Sie das Kontrollkästchen **Einstellungen des BlackBerry Gatekeeping Service überschreiben**, um jeden BlackBerry Gatekeeping Service in der Servergruppe zu deaktivieren.
7. Wenn für BlackBerry Secure Connect Plus andere DNS-Einstellungen als die Standardeinstellungen (**Einstellungen > Infrastruktur > BlackBerry Secure Connect Plus**) verwendet werden sollen, aktivieren Sie das Kontrollkästchen **DNS-Server überschreiben**. Gehen Sie wie folgt vor:
   a) Klicken Sie im Abschnitt **DNS-Server** auf +. Geben Sie die Adresse des DNS-Servers in Dezimalschreibweise mit Punkt ein (zum Beispiel: 192.0.2.0). Klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt so häufig wie nötig.
   b) Klicken Sie im Abschnitt **DNS-Suchsuffix** auf +. Geben Sie die das DNS-Suchsuffix ein (z. B. domain.com). Klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt so häufig wie nötig.
8. Wenn Sie die Protokollierungseinstellungen für die BlackBerry Connectivity Node-Instanzen in der Servergruppe konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Protokollierungseinstellungen überschreiben**. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie in der Dropdownliste **Fehlerbehebungsebenen des Serverprotokolls** die entsprechende Protokollebene aus.
   - Wenn Protokollereignisse an einen Syslog-Server weitergeleitet werden sollen, aktivieren Sie das Kontrollkästchen **Syslog**, und geben Sie den Hostnamen und den Port des Syslog-Servers an.
   - Wenn Sie lokale Protokolleinstellungen ändern möchten, aktivieren Sie das Kontrollkästchen **Lokalen Speicherpfad aktivieren**. Geben Sie die Größenbeschränkung (in MB) und die Altersgrenze (in Tagen) an, und wählen Sie aus, ob Sie Protokollordner komprimieren möchten.
   - Wenn Sie verschiedene Protokollebenen für BlackBerry Connectivity Node-Komponenten konfigurieren möchten, klicken Sie im Abschnitt **Dienstprotokoll überschreiben** auf +, und wählen Sie die entsprechende Komponente und Protokollebene aus. Wiederholen Sie diesen Schritt so häufig wie nötig.
9. Wenn Sie die Instanzen in der Servergruppe nur für einen Verbindungstyp verwenden möchten, aktivieren Sie das Kontrollkästchen **Leistungsmodus für einzelnen Dienst aktivieren**. Wählen Sie im Dropdown-Menü **Verbindungstyp** den Verbindungstyp aus (nur BlackBerry Secure Connect Plus, nur BlackBerry Secure Gateway oder nur BlackBerry Proxy).
10. Wenn Sie die BlackBerry Secure Gateway-Einstellungen für die Instanzen in der Servergruppe konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Einstellungen für BlackBerry Secure Gateway überschreiben**. Für iOS-Geräte, die eine moderne Authentifizierung verwenden, um eine Verbindung zu Microsoft Exchange Online herzustellen, müssen Sie den Erkennungsendpunkt und die E-Mail-Server-Ressource angeben:
    a) Aktivieren Sie das Kontrollkästchen **OAuth für E-Mail-Server-Authentifizierung aktivieren**.
    b) Geben Sie im Feld **Erkennungsendpunkt** die URL an, die für Erkennungsanforderungen verwendet werden soll. Die URL sollte folgendes Format haben: https://<*identity provider*>/.well-known/openid-configuration (z. B. `https://login.microsoftonline.com/common/.well-known/openid-configuration`) oder `https://login.windows.net/common/.well-known/openid-configuration`).
    c) Geben Sie im Feld **E-Mail-Server-Ressource** die URL der E-Mail-Server-Ressource an, die für Autorisierungs- und Tokenanforderungen mit OAuth verwendet werden soll. Beispiel: `https://outlook.office365.com`.

11. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Wählen Sie die Servergruppe aus, und klicken Sie auf , um BlackBerry Connectivity Node-Instanzen hinzuzufügen. Sie können jederzeit eine Instanz zu einer Servergruppe hinzufügen oder aus einer Servergruppe entfernen.

Fehlerbehebung: BlackBerry Connectivity Node

Problem	Mögliche Lösung
Keine gleichzeitige Aktivierung von BlackBerry Connectivity Node und UEM Cloud.	• Überprüfen Sie, ob die letzte Aktivierungsdatei, die Sie in der Verwaltungskonsole erstellt haben, hochgeladen wurde. Nur die letzte Aktivierungsdatei ist gültig. • Eine Aktivierungsdatei läuft nach 60 Minuten ab. Erstellen Sie eine neue Aktivierungsdatei, laden Sie sie hoch und führen Sie den Aktivierungsvorgang erneut durch. • Siehe KB 38964.

Keine Verbindung zwischen BlackBerry Connectivity Node und UEM Cloud.	• Überprüfen Sie, ob die folgenden ausgehenden Ports in der Firewall Ihres Unternehmens geöffnet sind, sodass die BlackBerry Connectivity Node-Komponenten (und ggf. zugeordnete Proxy-Server) mit der BlackBerry Infrastructure kommunizieren können (*region*.bbsecure.com):
	  • 443 (HTTPS) zum Aktivieren des BlackBerry Connectivity Node
	  • 3101 (TCP) für alle übrigen ausgehenden Verbindungen
	• Entnehmen Sie der letzten Protokolldatei Einzelheiten darüber, weshalb das Herstellen einer Verbindung zwischen BlackBerry Connectivity Node und UEM Cloud nicht möglich ist. Standardmäßig befinden sich die Protokolldateien unter *<drive:>*:\Programme \BlackBerry\BlackBerry Connectivity Node\Logs.

Problem	Mögliche Lösung
Keine Verbindung zwischen BlackBerry Connectivity Node und dem Unternehmensverzeichnis.	• Wenn Sie mehrere Instanzen von BlackBerry Connectivity Node verwenden, überprüfen Sie, ob alle dieselbe Version haben. • Überprüfen Sie, ob die Einstellungen für das Unternehmensverzeichnis korrekt sind. • Vergewissern Sie sich, dass alle Instanzen eine Verzeichnisverbindung haben und dass die Verzeichnisverbindungen auf allen Instanzen gleich konfiguriert sind. • Überprüfen Sie, ob die Anmeldeinformationen für das Verzeichniskonto korrekt sind und die erforderlichen Zugriffsrechte für das Unternehmensverzeichnis vorhanden sind. • Überprüfen Sie, ob die richtigen Ports in der Firewall Ihres Unternehmens geöffnet sind. • Stellen Sie sicher, dass für die beiden separaten Installationen nicht dieselbe Aktivierungsdatei verwendet wurde. • Stellen Sie sicher, dass die neueste Aktivierungsdatei verwendet wird. • Entnehmen Sie der letzten Protokolldatei Einzelheiten darüber, weshalb der Zugriff auf das Unternehmensverzeichnis über den BlackBerry Connectivity Node nicht möglich ist. Standardmäßig befinden sich die Protokolldateien unter <*drive:*>:\Programme \BlackBerry\BlackBerry Connectivity Node\Logs. • Wenn Sie Microsoft Active Directory verwenden, finden Sie weitere Informationen in KB 36955.

Konfigurieren von BlackBerry UEM zum Senden von Daten über einen Proxyserver

Sie können die folgenden Proxy-Konfigurationen in Ihrer BlackBerry UEM-Umgebung verwenden:

Umgebung	Proxy-Optionen
Lokales UEM	Sie können UEM so konfigurieren, dass Daten zuerst über einen TCP-Proxyserver gesendet werden, bevor sie die BlackBerry Infrastructure erreichen. Standardmäßig stellt 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 einen TCP-Proxyserver installieren. Der TCP-Proxyserver fungiert als Vermittler zwischen UEM und der BlackBerry Infrastructure. Sie können einen Proxyserver außerhalb der Unternehmens-Firewall in einer DMZ installieren. Durch die Installation eines TCP-Proxyservers in einer DMZ wird die Sicherheit für UEM zusätzlich erhöht. Nur der Proxyserver stellt von außerhalb der Firewall eine Verbindung zu UEM her. Alle Verbindungen zur BlackBerry Infrastructure zwischen UEM und den Geräten werden über den Proxyserver geleitet.
UEM Cloud	Um einen Proxyserver mit BlackBerry Connectivity Node zu verwenden, können Sie den BlackBerry Router als Proxyserver installieren oder einen bereits in der Umgebung Ihres Unternehmens installierten TCP-Proxyserver verwenden. Sie können den BlackBerry Router oder einen Proxyserver außerhalb der Unternehmens-Firewall in einer DMZ installieren. Durch die Installation des BlackBerry Router oder eines TCP-Proxyservers in einer DMZ wird die Sicherheit zusätzlich erhöht. Nur der BlackBerry Router oder der Proxyserver stellt von außerhalb der Firewall eine Verbindung zu BlackBerry Connectivity Node her. Alle Verbindungen zur BlackBerry Infrastructure zwischen BlackBerry Connectivity Node und den Geräten werden über den Proxyserver geleitet. Standardmäßig stellt BlackBerry Connectivity Node 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-Proxyserver fungiert als Vermittler zwischen BlackBerry Connectivity Node und der BlackBerry Infrastructure.

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

In lokalen UEM-Umgebungen können Sie einen transparenten TCP-Proxyserver für den BlackBerry UEM Core-Dienst konfigurieren. Dieser Dienst erfordert 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.

In UEM Cloud-Umgebungen sendet der BlackBerry Connectivity Node Aktivierungsdaten über Port 443 (HTTPS). Nach der Aktivierung sendet und empfängt der BlackBerry Connectivity Node Daten über Port 3101 (TCP). Sie können den BlackBerry Connectivity Node so konfigurieren, dass HTTPS- oder TCP-Daten über einen Proxy-Server weitergeleitet werden, der sich hinter der Firewall Ihres Unternehmens befindet. Die Authentifizierung mit einem Proxy-Server wird vom BlackBerry Connectivity Node nicht unterstützt.

Sie können jedoch mehrere TCP-Proxy-Server, die mit SOCKS v5 (keine Authentifizierung) konfiguriert wurden, für die Verbindung mit 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.

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 UEM-Domäne.

1. Befolgen Sie die Schritte für Ihre Umgebung:

Umgebung	Schritte
Lokales UEM	**a.** Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Infrastruktur > BlackBerry Router und Proxy**. **b.** Wählen Sie unter **Globale Einstellungen** die Option **Proxyserver**. **c.** Geben Sie für jeden Dienst, für den Sie den Proxyserver verwenden möchten, den FQDN oder die IP-Adresse und die Portnummer des Proxyservers an. In jedes Feld muss ein einzelner Wert eingegeben werden.
UEM Cloud	**a.** Klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Proxy**. **b.** Wählen Sie **Proxyserver**. **c.** Wenn Sie HTTPS-Aktivierungsdaten für den BlackBerry Connectivity Node über einen Proxy-Server leiten möchten, geben Sie in die Felder **Anmeldungs-Proxy** den FQDN oder die IP-Adresse und die Portnummer des Proxyservers ein. Der Proxyserver muss Daten über Port 443 an *<region>*.bbsecure.com senden können. **d.** Wenn Sie ausgehende Verbindungen von den Komponenten von BlackBerry Connectivity Node über einen Proxyserver senden möchten, geben Sie in die entsprechenden Felder den FQDN oder die IP-Adresse und die Portnummer des Proxyservers ein. Der Proxy-Server muss Daten über Port 3101 an *<region>*.bbsecure.com senden können.

2. 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 UEM-Domäne.

1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie bei einer lokalen UEM-Umgebung in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Infrastruktur > BlackBerry Router und Proxy**.

- Klicken Sie bei einer UEM Cloud-Umgebung in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Proxy**.

2. Wählen Sie **Proxyserver**.
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 2 bis 6 für jeden zu konfigurierenden SOCKS v5-Proxy-Server.
8. Geben Sie im Feld **Port** die Portnummer ein.
9. Klicken Sie auf **Speichern**.

Installieren eines eigenständigen BlackBerry Router in einer UEM Cloud-Umgebung

Der BlackBerry Router ist eine optionale Komponente, die Sie in einer DMZ außerhalb der Firewall Ihres Unternehmens installieren können. Der BlackBerry Router baut eine Verbindung mit dem Internet auf, um Daten zwischen BlackBerry Connectivity Node und Geräten zu senden, die die BlackBerry Infrastructure verwenden. Der BlackBerry Router agiert als Proxy-Server und kann SOCKS v5 (keine Authentifizierung) unterstützen.

Sie können mehrere Instanzen des BlackBerry Router für hohe Verfügbarkeit konfigurieren. Sie konfigurieren nur einen Port für die Überwachung durch BlackBerry Router-Instanzen. Standardmäßig stellt BlackBerry Connectivity Node über Port 3102 eine Verbindung mit dem BlackBerry Router her. Der BlackBerry Router unterstützt den gesamten ausgehenden Datenverkehr von den BlackBerry Connectivity Node-Komponenten.

Bevor Sie beginnen:

- Sie müssen einen eigenständigen BlackBerry Router auf einem Computer installieren, der keine Instanz des BlackBerry Connectivity Node hostet.
- Stellen Sie sicher, dass Sie den Namen des SRP-Hosts kennen. Der Name des SRP-Hosts lautet normalerweise `<country code>.srp.blackberry.com` (zum Beispiel `us.srp.blackberry.com`).

1. Klicken Sie in der Menüleiste der UEMVerwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup**.
2. Klicken Sie auf .
3. Klicken Sie auf **Download**.
4. Beantworten Sie auf der Seite für den Softwaredownload die erforderlichen Fragen, und klicken Sie auf **Download**. Speichern und entpacken Sie das Installationspaket.
5. Entpacken Sie im Ordner **Router** die ZIP-Datei **setupinstaller**. Diese ZIP-Datei enthält den Ordner **Installer** mit der Datei **Setup.exe**, die Sie zur Installation von BlackBerry Router verwenden.
6. Übertragen Sie die Datei **Setup.exe** auf den Computer, auf dem Sie den BlackBerry Router installieren möchten, und doppelklicken Sie sie, um die Setupanwendung auszuführen.

   Die Installation läuft im Hintergrund und zeigt keine Dialogfelder an. Sobald die Installation abgeschlossen ist, erscheint im Fenster „Dienste“ der BlackBerry Router-Dienst.
7. Klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Proxy**.
8. Wählen Sie **BlackBerry Router** aus.
9. Klicken Sie auf +.

10. Geben Sie die IP-Adresse oder den Hostnamen der BlackBerry Router-Instanz ein, zu der UEM eine Verbindung herstellen soll.
11. Klicken Sie auf **Hinzufügen**.
12. Geben Sie in das Feld **Port** die Portnummer ein, die von allen BlackBerry Router-Instanzen überwacht wird. Der Standardwert ist 3102.
13. Klicken Sie auf **Speichern**.

Konfigurieren von Verbindungen über interne Proxyserver

Wenn Ihr Unternehmen einen Proxyserver für Verbindungen zwischen Servern innerhalb Ihres Netzwerks verwendet, müssen Sie Ihre lokale BlackBerry UEM-Umgebung möglicherweise folgendermaßen konfigurieren:

- Lassen Sie zu, dass UEM Core mit der Verwaltungskonsole kommuniziert, wenn diese auf einem separaten Computer installiert ist.
- Lassen Sie zu, dass UEM mit anderen internen Diensten, wie Zertifizierungsstellen und Servern, die Push-Anwendungen hosten, kommuniziert.

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

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Infrastruktur > Serverseitiger Proxy**.
2. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Schritte
Konfigurieren Sie globale Proxyeinstellungen für die meisten oder alle Server in Ihrer UEM-Domäne.	**a.** Erweitern Sie **Globale serverseitige Proxy-Einstellungen**. **b.** Klicken Sie in der Dropdown-Liste **Typ** auf **PAC-Konfiguration** oder **Manuelle Konfiguration**. **c.** Füllen Sie die erforderlichen Felder aus. **d.** Klicken Sie auf **Speichern**.
Konfigurieren Sie Proxyeinstellungen für einen oder mehrere Server, die sich von den globalen Proxyeinstellungen unterscheiden.	**a.** Erweitern Sie den Servernamen. **b.** Klicken Sie in der Dropdown-Liste **Typ** auf **Keinen**, **PAC-Konfiguration** oder **Manuelle Konfiguration**. **c.** Füllen Sie die erforderlichen Felder aus. **d.** Klicken Sie auf **Speichern**.

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

Sie müssen BlackBerry UEM lokal mit einem SMTP-Server verbinden, damit es Aktivierungsanweisungen, Warnmeldungen zur Vorschrifteneinhaltung auf Geräten, Kennwörter für UEM Self-Service und E-Mail-Benachrichtigungen an Gerätebenutzer senden kann.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole 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 -E-Mail-Benachrichtigungen von UEM verwendet werden soll (z. B. `donotreply` oder `UEM Admin`).
4. Geben Sie in das Feld **Absenderadresse** die E-Mail-Adresse ein, die UEM zum Senden von E-Mail-Benachrichtigungen verwenden soll.
5. Geben Sie in das Feld **SMTP-Server** den FQDN des SMTP-Servers ein.
6. Geben Sie im Feld **SMTP-Serverport** die Portnummer des SMTP-Servers ein. Die Standardportnummer ist 25.
7. Klicken Sie in der Dropdown-Liste **Unterstützter Verschlüsselungstyp** auf den entsprechenden Typ.
8. Wenn für den SMTP-Server eine Authentifizierung erforderlich ist, geben Sie den Benutzernamen und das Kennwort an.
9. Importieren Sie ggf. ein SMTP-Zertifizierungsstellenzertifikat:
   a) Kopieren Sie die SSL-Zertifikatdatei für den SMTP-Server Ihres Unternehmens auf den von Ihnen verwendeten Computer.
   b) Klicken Sie auf **Durchsuchen**.
   c) Navigieren Sie zur SSL-Zertifikatdatei, 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. UEM sendet die Nachricht an die von Ihnen im Feld **Absenderadresse** festgelegte E-Mail-Adresse.

Herstellen einer Verbindung zu Unternehmensverzeichnissen

Sie können BlackBerry UEM mit dem Unternehmensverzeichnis Ihres Unternehmens verbinden, um die folgenden Funktionen zu nutzen:

- Sie können in UEM mit Benutzerdaten aus dem Verzeichnis Benutzerkonten erstellen, und UEM kann Administratoren für die Verwaltungskonsole und Benutzer für BlackBerry UEM Self-Service authentifizieren.
- Sie können Unternehmensverzeichnisgruppen mit UEM-Gruppen verknüpfen, um Benutzer auf die gleiche Weise wie in Ihrem Unternehmensverzeichnis zu organisieren und die Zuweisung und Verwaltung von IT-Richtlinien, Profilen und Apps für Benutzer zu vereinfachen. Diese werden als verzeichnisverknüpfte Gruppen bezeichnet.
- Sie haben die Möglichkeit, für bestimmte Gruppen in Ihrem Unternehmensverzeichnis, Onboarding zu aktivieren, um UEM-Benutzer automatisch erstellen zu lassen. Diese werden als Onboarding-Verzeichnisgruppen bezeichnet. Wenn Sie neue Benutzer zu diesen Verzeichnisgruppen hinzufügen, werden neue Benutzerkonten für diese Benutzer in UEM erstellt. Wenn Sie Onboarding aktivieren, können Sie mithilfe von Offboarding-Konfigurationen auch Gerätedaten oder UEM-Benutzerkonten löschen, wenn Benutzer aus Gruppen in Ihrem Unternehmensverzeichnis entfernt oder deaktiviert werden.

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

Schritt	Aktion
1	In einer lokalen UEM-Umgebung, Verbindung zu einer Microsoft Active Directory-Instanz oder Herstellen der Verbindung zu einem LDAP-Verzeichnis. Installieren und konfigurieren Sie in einer UEM Cloud-Umgebung die BlackBerry Connectivity Node, um eine Verbindung zu Ihrem Unternehmensverzeichnis herzustellen. Anweisungen zum lokalen Verbinden von UEM oder zum Verbinden von UEM Cloud mit Entra ID finden Sie unter Verbinden von BlackBerry UEM mit Entra ID, um Verzeichnisbenutzerkonten zu erstellen.
2	Optional Aktivieren von per Verzeichnis verknüpften Gruppen.
3	Optional Aktivieren und Konfigurieren von Onboarding und Offboarding.
4	Konfigurieren Sie optional die Verzeichnissynchronisierung.

Verbindung zu einer Microsoft Active Directory-Instanz

Die folgende Aufgabe gilt für eine lokale UEM-Umgebung. Installieren und konfigurieren Sie in einer UEM Cloud-Umgebung die BlackBerry Connectivity Node, um eine Verbindung zu Ihrem Unternehmensverzeichnis herzustellen.

Bevor Sie beginnen:

- Erstellen Sie ein Microsoft Active Directory-Konto, das von 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.
  - Der UEM-Server muss auch mit der Active Directory-Domäne verbunden sein.
- Wenn Ihr Unternehmen eine Microsoft Exchange-Ressourcengesamtstruktur verwendet, müssen Sie für jedes Benutzerkonto ein Postfach in der Ressourcenstruktur erstellen und diese mit den Benutzerkonten in der Kontengesamtstruktur verknüpfen. UEM verwendet die Postfächer, um die Benutzerkonten in den einzelnen Domänen zu suchen. Um Benutzer zu authentifizieren, die sich bei UEM anmelden, muss UEM die Benutzerinformationen lesen, die auf den zur Ressourcengesamtstruktur gehörenden globalen Katalogservern gespeichert sind. Sie müssen ein Microsoft Active Directory-Konto für UEM erstellen, das sich in einer Windows-Domäne befindet, die Teil der Ressourcengesamtstruktur ist. Beim Erstellen der Verzeichnisverbindung geben Sie die Windows-Anmeldeinformationen für das Microsoft Active Directory-Konto und ggf. die Namen der globalen Katalogserver an, die UEM nutzen kann.

1. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf + > **Verbindung zu Microsoft Active Directory**.
3. Geben Sie im Feld **Name der Verbindung des Verzeichnisses** einen Namen für die Verzeichnisverbindung ein.
4. Geben Sie im Feld **Benutzername** den Benutzernamen des Microsoft Active Directory-Kontos 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 UEM die Schlüsselverteilungscenter (KDCs) automatisch erkennen kann, klicken Sie auf **Automatisch**.
   - Um die Liste der KDCs anzugeben, die 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 UEM verwenden soll.
8. Führen Sie in der Dropdown-Liste **Auswahl des globalen Katalogs** eine der folgenden Aktionen aus:
   - Wenn UEM die globalen Katalogserver automatisch erkennen soll, klicken Sie auf **Automatisch**.
   - Um die Liste der globalen Katalogserver anzugeben, die UEM verwenden soll, klicken Sie auf **Manuell**. Geben Sie im Feld **Servernamen** den DNS-Namen des globalen Katalogservers ein, auf den 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 weitere 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 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 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 +. Klicken Sie im Feld **Domäne** auf die Domäne, 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 Active Directory-Konto in der ausgewählten Domäne angeben. Im Feld **KDC-Auswahl** können Sie „Automatisch“ auswählen, damit UEM Key Distribution Centers automatisch sucht. Wenn Sie „Manuell“ auswählen, können Sie die für die Authentifizierung zu verwendende KDC-Liste für UEM selbst angeben. Klicken Sie auf **Hinzufügen**.

12. Wenn Ihre Umgebung eine Microsoft Exchange-Ressourcengesamtstruktur enthält und 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 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 UEM durchsuchen soll. Geben Sie bei Bedarf die globalen Katalogserver an, auf die 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 in der Dokumentation für Administratoren.

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:

- Führen Sie eine der folgenden optionalen Aufgaben aus:
  - Aktivieren von per Verzeichnis verknüpften Gruppen.
  - Aktivieren und Konfigurieren von Onboarding und Offboarding.
  - Konfigurieren der Verzeichnissynchronisierung.
- Wenn Sie eine Verzeichnisverbindung entfernen, werden alle Benutzer, die aus diesem Verzeichnis zu UEM hinzugefügt wurden, in lokale Benutzer konvertiert. Sobald Benutzer in lokale Benutzer umgewandelt wurden, können sie nicht wieder in verzeichnisgebundene Benutzer umgewandelt werden, selbst wenn Sie die Unternehmensverzeichnisverbindung später wieder hinzufügen. Benutzer werden weiterhin als lokale Benutzer fungieren, aber UEM kann keine Updates aus dem Unternehmensverzeichnis synchronisieren.

Herstellen der Verbindung zu einem LDAP-Verzeichnis

Die folgende Aufgabe gilt für eine lokale UEM-Umgebung. Installieren und konfigurieren Sie in einer UEM Cloud-Umgebung die BlackBerry Connectivity Node, um eine Verbindung zu Ihrem Unternehmensverzeichnis herzustellen.

Bevor Sie beginnen:

- Erstellen Sie ein LDAP-Konto für UEM im entsprechenden LDAP-Verzeichnis. Das Konto muss die folgenden Anforderungen erfüllen:
  - Das Konto muss über Leseberechtigungen für alle Benutzer im Verzeichnis verfügen.
  - Das Kennwort muss so konfiguriert werden, dass es nicht abläuft und dass es bei der nächsten Anmeldung nicht geändert werden muss.
- 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 UEM TLS 1.2 verwenden.
- Überprüfen Sie die von Ihrem Unternehmen verwendeten LDAP-Attributwerte (die nachstehenden Schritte enthalten Beispiele für typische Attributwerte). Sie benötigen diese für die folgenden Schritte.

1. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf + **> 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 **LDAP-Server-SSL-Zertifikat** 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 nach Benutzer** den LDAP-Suchfilter ein, der zum Auffinden von Benutzerobjekten auf Ihrem Unternehmensverzeichnisserver erforderlich ist. Geben Sie beispielsweise für ein IBM Domino Directory `(objectClass=Person)` ein.
10. Führen Sie in der Dropdown-Liste **LDAP-Benutzersuchbereich** 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). Beispiel: `dominoUNID`.
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 **Anmeldeattribute** 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 **Benutzerprinzipalname** den Benutzerprinzipalnamen für SCEP ein (beispielsweise `mail`).
18. Geben Sie im Feld **Abteilung** das Attribut für die Abteilung der einzelnen Benutzer ein.
19. Geben Sie im Feld **Berufsbezeichnung** das Attribut für die Berufsbezeichnung der einzelnen Benutzer ein.
20. Wenn Sie zusätzliche Felder aus dem LDAP-Verzeichnis synchronisieren möchten, aktivieren Sie das Kontrollkästchen **Zusätzliche Benutzerdetails synchronisieren**. Geben Sie bei Bedarf die Attribute für die zusätzlichen Felder ein.
21. Um per Verzeichnis verknüpfte Gruppen für die Verzeichnisverbindung zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktivieren von per Verzeichnis verknüpften Gruppen**.
    a) Geben Sie im Feld **Suchbasis für Gruppen** den Wert ein, der als Basis-DN für Gruppeninformationssuchen verwendet werden soll.
    b) Geben Sie im Feld **LDAP-Suchfilter für Gruppen** den LDAP-Suchfilter ein, der zum Auffinden von Gruppenobjekten in Ihrem Unternehmensverzeichnis erforderlich ist. Geben Sie z. B. für IBM Domino Directory `(objectClass=dominoGroup)` ein.
    c) 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 (beispielsweise `cn`).
    d) Geben Sie im Feld **Anzeigename der Gruppe** das Attribut für den Anzeigenamen der einzelnen Gruppen ein (z. B. `cn`).
    e) Geben Sie im Feld **Gruppenmitgliedschaft – Attribut** den Namen des Attributs für die Gruppenmitgliedschaft ein. Die Attributwerte müssen im DN-Format vorliegen (z. B. `CN=jsmith,CN=Users,DC=example,DC=com`).
    f) Geben Sie im Feld **Gruppenname testen** einen vorhandenen Gruppennamen ein, um die festgelegten Gruppenattribute zu validieren.
    g) Wenn Sie die Seitensuche für Gruppenmitglieder aktivieren möchten, aktivieren Sie das Kontrollkästchen **Seitensuche für Gruppen aktivieren**.
22. Klicken Sie auf **Speichern**.
23. Klicken Sie auf **Schließen**.

Wenn Sie fertig sind:

- Führen Sie eine der folgenden optionalen Aufgaben aus:
  - Aktivieren von per Verzeichnis verknüpften Gruppen.
  - Aktivieren und Konfigurieren von Onboarding und Offboarding.
  - Konfigurieren der Verzeichnissynchronisierung.
- Wenn Sie eine Verzeichnisverbindung entfernen, werden alle Benutzer, die aus diesem Verzeichnis zu UEM hinzugefügt wurden, in lokale Benutzer konvertiert. Sobald Benutzer in lokale Benutzer umgewandelt wurden, können sie nicht wieder in verzeichnisgebundene Benutzer umgewandelt werden, selbst wenn Sie die Unternehmensverzeichnisverbindung später wieder hinzufügen. Benutzer werden weiterhin als lokale Benutzer fungieren, aber UEM kann keine Updates aus dem Unternehmensverzeichnis synchronisieren.

Aktivieren von per Verzeichnis verknüpften Gruppen

Sie können Gruppen in BlackBerry UEM mit Gruppen in Ihrem Unternehmensverzeichnis verknüpfen, um Benutzer in UEM auf die gleiche Weise wie im Verzeichnis zu organisieren und die Zuweisung und Verwaltung von IT-Richtlinien, Profilen und Apps für Benutzer zu vereinfachen. Weitere Informationen finden Sie unter Erstellen und Verwalten von Benutzergruppen in der Dokumentation für Administratoren.

Bevor Sie beginnen:

- Herstellen einer Verbindung zum Unternehmensverzeichnis:
  - UEM lokal: Verbindung zu einer Microsoft Active Directory-Instanz oder Herstellen der Verbindung zu einem LDAP-Verzeichnis.
  - UEM Cloud: Installieren und Konfigurieren von BlackBerry Connectivity Node für die Verbindung mit Microsoft AD oder LDAP.
  - Lokal oder Cloud: Verbinden von UEM mit Microsoft Entra ID.
- 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 der Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf eine Unternehmensverzeichnis-Verbindung.
3. Aktivieren Sie auf der Registerkarte **Synchronisierungseinstellungen** das Kontrollkästchen **Aktivieren von per Verzeichnis verknüpften Gruppen**.
4. Wenn Sie die Synchronisierung von Unternehmensverzeichnisgruppen erzwingen möchten, 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.
5. Geben Sie im Feld **Synchronisierungsbeschränkung** die maximale Anzahl Änderungen ein, die pro Synchronisierungsprozess zulässig sein sollen.

   Falls die Anzahl der zu synchronisierenden Änderungen das Synchronisierungslimit übersteigt, können Sie die Ausführung der Synchronisierung verhindern. UEM ermittelt insgesamt die folgenden Änderungen: 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:

- Optional Aktivieren und Konfigurieren von Onboarding und Offboarding.
- Konfigurieren Sie optional die Verzeichnissynchronisierung.
- Erstellen Sie einer per Verzeichnis verknüpfte Gruppe. Weitere Informationen finden Sie unter Erstellen und Verwalten von Benutzergruppen in der Dokumentation für Administratoren.

Aktivieren und Konfigurieren von Onboarding und Offboarding

Wenn Sie Onboarding aktivieren, fügen Sie universelle oder globale Verzeichnisgruppen zu UEM als Onboarding-Verzeichnisgruppen hinzu (Onboarding wird für lokale Gruppen der Domäne nicht unterstützt). Wenn UEM während eines Synchronisierungsprozesses einen Verzeichnisbenutzer in einer Onboarding-Verzeichnisgruppe erkennt, der kein entsprechendes UEM-Benutzerkonto hat, wird dieses Benutzerkonto in UEM erstellt. Wenn Sie das Onboarding aktivieren, können Sie auch das Offboarding konfigurieren. Wenn Sie einen Benutzer aus einer Onboarding-Verzeichnisgruppe deaktivieren oder entfernen, kann UEM Gerätedaten löschen und den Benutzer aus UEM entfernen.

Hinweis: Wenn Offboarding aktiviert ist, werden alle UEM-Benutzerkonten, die nicht Mitglied einer Onboarding-Verzeichnisgruppe sind, unabhängig davon, wie sie zu UEM hinzugefügt wurden, während des nächsten Synchronisierungsprozesses entfernt.

Bevor Sie beginnen:

- Herstellen einer Verbindung zum Unternehmensverzeichnis:
  - UEM lokal: Verbindung zu einer Microsoft Active Directory-Instanz oder Herstellen der Verbindung zu einem LDAP-Verzeichnis.
  - UEM Cloud: Installieren und Konfigurieren von BlackBerry Connectivity Node für die Verbindung mit Microsoft AD oder LDAP.
  - Lokal oder Cloud: Verbinden von UEM mit Microsoft Entra ID.
- 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 der Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf eine Unternehmensverzeichnis-Verbindung.
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 eine der folgenden Aktionen aus:

Aufgabe	Schritte
Fügen Sie Onboarding-Verzeichnisgruppen hinzu, und konfigurieren Sie die Geräteaktivierungsoptionen.	**a.** Klicken Sie auf +. **b.** Suchen Sie nach universellen oder globalen Verzeichnisgruppen, und fügen Sie sie hinzu. **c.** Wählen Sie für jede Verzeichnisgruppe aus, ob verschachtelte Gruppen verknüpft werden sollen. **d.** Geben Sie im Abschnitt **Geräteaktivierung** an, ob integrierte Benutzer ein automatisch generiertes Aktivierungskennwort und eine E-Mail 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.

Aufgabe	Schritte
Benutzer hinzufügen, die nur BlackBerry Dynamics-Apps verwenden dürfen.	Führen Sie die folgenden Schritte aus, wenn Sie Benutzer hinzufügen möchten, die nur BlackBerry Dynamics-Apps verwenden. Diese Benutzer aktivieren ihre Geräte nicht auf UEM mit dem UEM Client, und ihre Geräte werden nicht von UEM verwaltet. **a.** Aktivieren Sie das Kontrollkästchen **Nur Benutzer mit BlackBerry Dynamics-Apps integrieren**. **b.** Klicken Sie auf +. **c.** Suchen Sie nach universellen oder globalen Verzeichnisgruppen, und fügen Sie sie hinzu. **d.** Wählen Sie für jede Verzeichnisgruppe aus, ob verschachtelte Gruppen verknüpft werden sollen. **e.** Wählen Sie die Anzahl der Zugriffsschlüssel aus, die pro Benutzer erzeugt werden sollen, die Ablauffrist des Zugriffsschlüssels und E-Mail-Vorlage.
Offboarding konfigurieren.	Wenn Sie Gerätedaten beim Offboarding eines Benutzers aus UEM löschen möchten, aktivieren Sie das Kontrollkästchen **Gerätedaten löschen, wenn der Benutzer von allen integrierten Verzeichnisgruppen entfernt wird**. Gehen Sie wie folgt vor: • Wählen Sie die entsprechende Option für die Daten aus, die Sie vom Gerät entfernen möchten. • Wenn Sie ein Benutzerkonto aus UEM entfernen möchten, wenn ein Benutzer aus allen Onboarding-Verzeichnisgruppen entfernt wird, aktivieren Sie das Kontrollkästchen **Benutzer löschen, wenn der Benutzer von allen integrierten Verzeichnisgruppen entfernt wird**. • Wenn Sie das Löschen von Benutzern und Gerätedaten um zwei Stunden nach einem Synchronisierungszyklus verzögern möchten, aktivieren Sie das Kontrollkästchen **Offboarding-Schutz**. Mit dieser Option kann unerwartetes Löschen aufgrund von Verzeichnisreplikationslatenz vermieden werden.

6. Wenn Sie die Synchronisierung von Unternehmensverzeichnisgruppen erzwingen möchten, 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.
7. Geben Sie im Feld **Synchronisierungsbeschränkung** die maximale Anzahl Änderungen ein, die pro Synchronisierungsprozess zulässig sein sollen.

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

Wenn Sie fertig sind: Konfigurieren Sie optional die Verzeichnissynchronisierung.

Synchronisieren einer Verzeichnisverbindung

Nachdem Sie UEM mit Ihrem Unternehmensverzeichnis verbunden haben, können Sie den Synchronisierungsprozess jederzeit manuell starten oder wiederkehrende Synchronisierungen planen. Sie können die Vorschau eines Synchronisierungsberichts vor der nächsten Synchronisierung anzeigen und den Bericht nach Abschluss eines Synchronisierungsprozesses anzeigen.

Bevor Sie beginnen:

- Herstellen einer Verbindung zum Unternehmensverzeichnis:
  - UEM lokal: Verbindung zu einer Microsoft Active Directory-Instanz oder Herstellen der Verbindung zu einem LDAP-Verzeichnis.
  - UEM Cloud: Installieren und Konfigurieren von BlackBerry Connectivity Node für die Verbindung mit Microsoft AD oder LDAP.
  - Lokal oder Cloud: Verbinden von UEM mit Microsoft Entra ID.
- Optional Aktivieren von per Verzeichnis verknüpften Gruppen und Aktivieren und Konfigurieren von Onboarding und Offboarding.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
Vorschau einer Synchronisierung.	**a.** Klicken Sie auf für die Verzeichnisverbindung, für die Sie eine Vorschau der Synchronisierung anzeigen möchten. **b.** Klicken Sie auf **Jetzt Vorschau anzeigen**. **c.** Wenn die Verarbeitung des Berichts abgeschlossen ist, klicken Sie auf das Datum in der Spalte **Letzter Bericht**.
Manuelles Starten einer Verzeichnissynchronisieru	**a.** Klicken Sie auf für die Verzeichnisverbindung, die Sie synchronisieren möchten. **b.** Wenn die Synchronisierung abgeschlossen ist, klicken Sie auf das Datum in der Spalte **Letzter Bericht**. **c.** Um eine CSV-Datei des Berichts zu exportieren, klicken Sie auf .

Aufgabe	Schritte
Hinzufügen eines Synchronisierungsplans.	**a.** Klicken Sie auf die Verzeichnisverbindung, für die Sie die Synchronisierung planen möchten. **b.** Klicken Sie auf der Registerkarte **Synchronisierungszeitplan** auf +. **c.** Wählen Sie in der Dropdown-Liste **Synchronisierungstyp** eine der folgenden Optionen aus: • **Alle Gruppen und Benutzer**: Das Onboarding und Offboarding der Benutzer erfolgt nach Bedarf, Änderungen der Gruppenmitgliedschaft werden synchronisiert, und Änderungen an Benutzerattributen werden synchronisiert. • **Onboarding-Gruppen**: Das Onboarding und Offboarding der Benutzer erfolgt nach Bedarf, und Änderungen an Benutzerattributen werden synchronisiert. • **Per Verzeichnis verknüpfte Gruppen**: Änderungen der Gruppenmitgliedschaft werden synchronisiert, und Änderungen an Benutzerattributen werden synchronisiert. • **Benutzerattribute**: Nur Änderungen an Benutzerattributen werden synchronisiert. **d.** Wählen Sie in der Dropdown-Liste **Wiederholung** die entsprechende Option aus, und konfigurieren Sie die Wiederholungseinstellungen nach Bedarf. **e.** Klicken Sie auf **Hinzufügen**. **f.** Klicken Sie auf **Speichern**.

Verbinden von BlackBerry UEM mit Entra ID, um Verzeichnisbenutzerkonten zu erstellen

Sie können eine Verbindung zwischen BlackBerry UEM und Microsoft Entra ID herstellen, um Verzeichnisbenutzerkonten in UEM zu erstellen. Nachdem Sie die Verbindung konfiguriert haben, können Sie Benutzerdaten aus dem Verzeichnis suchen und zum Erstellen von UEM-Benutzern importieren. Verzeichnisbenutzer können ihre Verzeichnisanmeldeinformationen für den Zugriff auf BlackBerry UEM Self-Service verwenden. Wenn Sie einem Verzeichnisbenutzern eine Administratorrolle zuweisen, kann der Benutzer sich auch mit seinen Verzeichnisanmeldedaten bei der Verwaltungskonsole anmelden.

Wenn Ihr Unternehmen ein lokales Active Directory verwendet und Konten mit Entra ID synchronisiert werden, sollten Sie stattdessen eine Verzeichnisverbindung für Ihr lokales Active Directory erstellen (siehe Verbindung zu einer Microsoft Active Directory-Instanz). Eine Verbindung zwischen UEM und Entra ID ist geeignet, wenn Entra ID Ihr primärer Verzeichnisdienst ist und Sie nicht über ein lokales Active Directory verfügen.

Hinweis: Nach dem Verbinden von UEM mit Entra ID ändern sich die UEM-Konsolen-URLs wie folgt ("&redirect=no" wird vom Ende der URL entfernt):

- Verwaltungskonsole: https://<*server_name*>:<*port*>/admin/index.jsp?tenant=<*tenant_ID*>
- Self-Service-Konsole: https://<*server_name*>:<*port*>/mydevice/index.jsp?tenant=<*tenant_ID*>

Bevor Sie beginnen: Sie müssen über ein Microsoft Entra ID-Konto verfügen. Wenn Sie noch kein Konto haben, gehen Sie auf https://azure.microsoft.com,, um ein Konto zu erstellen. Verwenden Sie dieses Konto, um sich beim Entra-Portal anzumelden.

1. Melden Sie sich im Entra-Portal an.
2. Fügen Sie im Abschnitt für Entra ID-App-Registrierungen eine neue Registrierung hinzu.
3. Geben Sie Folgendes an, und schließen Sie die Registrierung ab:
   a) Geben Sie einen Namen für die Registrierung ein.
   b) Wählen Sie aus, welche Kontotypen die Anwendung verwenden oder auf die API zugreifen können.
   c) Klicken Sie für die Umleitungs-URI auf **Web**, und geben Sie `http://localhost` ein.
4. Kopieren Sie die Anwendungs-ID.
   Dies ist die Client-ID, mit der Sie sich bei UEM registrieren.
5. Fügen Sie im Abschnitt zum Verwalten von API-Berechtigungen (Schaltfläche „Registrieren“) eine Berechtigung hinzu, und wählen Sie Folgendes aus:
   - **Microsoft Graph**
   - **Anwendungsberechtigungen**
   - Legen Sie die folgenden Berechtigungen fest: **Group.Read.All (Anwendung)**, **User.Read (delegiert)**, **User.Read.All (Anwendung)**
6. Erteilen Sie die Zustimmung des Administrators für alle Konten im aktuellen Verzeichnis.
7. Fügen Sie im Abschnitt zur Verwaltung von Zertifikaten und geheimen Schlüsseln einen neuen Client-Schlüssel hinzu, und geben Sie eine Beschreibung und Dauer an.
8. Kopieren Sie das Feld „Wert“ des neuen Client-Schlüssels (keine Schlüssel-ID).
   Dies ist der Client-Schlüssel, mit dem Sie sich bei UEM registrieren.
9. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
10. Klicken Sie auf + > **Verbindung zu Microsoft Entra ID**.
11. Geben Sie im Feld **Name der Verbindung des Verzeichnisses** einen Namen für die Verbindung ein.
12. Geben Sie im Feld **Domäne** die Entra ID-Domäne ein.

13. Geben Sie im Feld **Client-ID** die ID ein, die Sie in Schritt 4 aufgezeichnet haben.

14. Geben Sie in das Feld **Client-Schlüssel** den Wert ein, den Sie in Schritt 8 aufgezeichnet haben.

15. Klicken Sie auf **Fortfahren**.

16. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Sie können eine der folgenden optionalen Aufgaben ausführen:

- Aktivieren von per Verzeichnis verknüpften Gruppen
- Aktivieren und Konfigurieren von Onboarding und Offboarding
- Synchronisieren einer Verzeichnisverbindung

Konfigurieren von BlackBerry UEM zur Verwaltung von Microsoft Intune-App-Schutzprofilen

Wenn Sie BlackBerry UEM zum Erstellen, Verwalten und Zuweisen von Microsoft Intune-App-Schutzprofilen verwenden möchten, um Daten in Office 365-Apps zu schützen, müssen Sie Folgendes tun:

Schritt	Aktion
1	Lesen Sie Voraussetzungen zur Unterstützung des Intune-App-Schutzes.
2	Erstellen einer App-Registrierung in Entra.
3	Konfigurieren von BlackBerry UEM für die Synchronisierung mit Microsoft Intune.

Voraussetzungen zur Unterstützung des Intune-App-Schutzes

- Um BlackBerry UEM mit Intune zu synchronisieren, müssen Sie ein Microsoft-Administratorkonto mit einer Intune-Lizenz und einer der folgenden Berechtigungen im Entra-Portal verwenden: globaler Administrator, eingeschränkter Administrator mit Intune-Dienstadministratorrolle oder eine benutzerdefinierte Rolle mit den in KB 50341 beschriebenen Berechtigungen.
- Benutzerkonten, denen Sie Intune-App-Schutzprofile zuweisen möchten, müssen in Entra ID vorhanden sein.
- Benutzer müssen als Verzeichnisbenutzer zu UEM hinzugefügt werden.
- Wenn Sie Ihr lokales Microsoft Active Directory integriert haben, müssen Benutzer mit Entra ID synchronisiert werden. Weitere Informationen finden Sie in der Microsoft-Dokumentation für Entra ID Connect.

Erstellen einer App-Registrierung in Entra

Sie müssen eine App-Registrierung in Entra erstellen, die UEM zur Authentifizierung mit Entra verwendet werden kann.

Bevor Sie beginnen:

- Lesen Sie Voraussetzungen zur Unterstützung des Intune-App-Schutzes.
- Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > Microsoft Intune**. Notieren Sie den Wert der **Antwort-URL**. Sie verwenden diese URL in Schritt 3.

1. Melden Sie sich im Entra-Portal an.
2. Fügen Sie im Abschnitt für App-Registrierungen eine neue Registrierung hinzu.
3. Geben Sie Folgendes an, und schließen Sie die Registrierung ab:
   a) Geben Sie einen Namen für die Registrierung ein.
   b) Wählen Sie aus, welche Kontotypen die Anwendung verwenden oder auf die API zugreifen können.
   c) Klicken Sie für die Umleitungs-URI auf **Mobile Client/Desktop**, und geben Sie die Antwort-URL von der Verwaltungskonsole ein.
4. Kopieren Sie die Anwendungs-ID.

Dies ist die Client-ID, mit der Sie sich bei UEM registrieren.

5. Fügen Sie im Abschnitt zum Verwalten von API-Berechtigungen eine Berechtigung hinzu, und wählen Sie Folgendes aus:
   - **Microsoft Graph**
   - **Delegierte Berechtigungen**
   - Legen Sie die folgenden delegierten Berechtigungen 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)**
6. Erteilen Sie die Zustimmung des Administrators für alle Konten im aktuellen Verzeichnis.
7. Fügen Sie im Abschnitt zur Verwaltung von Zertifikaten und geheimen Schlüsseln einen neuen Client-Schlüssel hinzu, und geben Sie eine Beschreibung und Dauer an.
8. Kopieren Sie das Feld „Wert“ des neuen Client-Schlüssels (keine Schlüssel-ID).

   Dies ist der Client-Schlüssel, mit dem Sie sich bei UEM registrieren.

Wenn Sie fertig sind: Konfigurieren von BlackBerry UEM für die Synchronisierung mit Microsoft Intune.

Konfigurieren von BlackBerry UEM für die Synchronisierung mit Microsoft Intune

Bevor Sie beginnen: Erstellen einer App-Registrierung in Entra.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Microsoft Intune**.
2. Geben Sie im Feld **Entra-Mandanten-ID** die ID des Entra ID-Mandanten Ihres Unternehmens ein.
3. Geben Sie im Feld **Client-ID** die ID ein, die Sie unter Erstellen einer App-Registrierung in Entra aufgezeichnet haben.
4. Geben Sie in das Feld **Client-Schlüssel** den Wert ein, den Sie unter Erstellen einer App-Registrierung in Entra aufgezeichnet haben.
5. Klicken Sie auf **Weiter**.
6. Geben Sie die Zugangsdaten des Intune-Administratorkontos an, das Sie für den Synchronisierungsprozess verwenden möchten.

Wenn Sie fertig sind:

- Weitere Informationen finden Sie unter Verwalten von durch Microsoft Intune geschützten Apps in der Dokumentation für Administratoren.
- Wenn Sie die Anmeldeinformationen des Intune-Administratorkontos erneut eingeben müssen (z. B. Kennwortänderung), klicken Sie unter **Einstellungen > Externe Integration > Microsoft Intune** auf **Anmeldeinformationen aktualisieren**.

Konfigurieren von BlackBerry UEM als Intune-Konformitätspartner in Entra

Wenn Sie den bedingten Zugriff mit Entra ID für Ihr Unternehmen konfiguriert haben, können Sie BlackBerry UEM als Konformitätspartner konfigurieren, sodass iOS- und Android-Geräte, die von UEM verwaltet werden, von Intune als vertrauenswürdig erkannt werden, wenn Sie auf Cloud-basierte Apps wie Office 365 zugreifen.

Sie können mehr als einen UEM-Mandanten für jeden Entra-Mandanten konfigurieren, aber alle UEM-Mandanten verwenden denselben Eintrag für die Partner-Konformitätsverwaltung. Entra kann nicht unterscheiden, von welchem UEM-Mandanten ein Kompatibilitätsstatus-Update stammt. Sie können den UEM-Mandanten so konfigurieren, dass er eine Verbindung zu einem oder mehreren Entra-Mandanten herstellt. Sie müssen eine Verzeichnisverbindung zu UEM hinzufügen, und zwar für jeden Entra-Mandanten.

Wenn Benutzer ihre Geräte auf UEM aktivieren, meldet UEM den Geräte-Konformitätsstatus an Entra. Die Konformitätsanforderung wird erfüllt, ohne dass Geräte direkt bei Intune registriert werden müssen. UEM benachrichtigt Entra, wenn ein Gerät nicht konform ist und wenn ein Gerät wieder konform wird.

Wenn Sie die bedingte Zugriffskontrolle „Gerät muss als konform markiert werden“ in Entra nicht verwenden möchten, und wenn Sie vertrauenswürdige Speicherorte verwenden möchten, um den Zugriff von Geräten innerhalb Ihres Netzwerks zu steuern, können Sie dies in UEM erreichen, indem Sie den Datenverkehr an Microsoft-Dienste weiterleiten. Dies erfolgt über die BlackBerry Connectivity Node-Instanzen Ihres Unternehmens. In diesem Szenario müssen Sie die Anweisungen in diesem Abschnitt nicht befolgen, um UEM mit Entra ID zu verbinden und einen bedingten Zugriff zu erhalten.

Voraussetzungen für die Konfiguration des bedingten Zugriffs in Entra ID.

- Stellen Sie sicher, dass Sie über ein Microsoft-Konto mit einer Intune-Lizenz und einer der folgenden Berechtigungen im Entra-Portal verfügen: globaler Administrator, eingeschränkter Administrator mit Intune-Dienstadministratorrolle oder eine benutzerdefinierte Rolle mit den in KB 50341 beschriebenen Berechtigungen.
- Fügen Sie im Microsoft Endpoint Manager Admin Center, im Abschnitt für Partner-Konformitätsverwaltung, **BlackBerry UEM Entra Conditional Access** als Konformitätspartner für iOS- und Android-Geräte hinzu, und weisen Sie die Einstellung Benutzern und Gruppen zu.
- Erstellen und konfigurieren Sie in Entra ID ein Profil für den bedingten Zugriff, und aktivieren Sie die Option „Gerät muss als konform markiert werden“. Beachten Sie, dass dies die einzige Profileinstellung für bedingten Zugriff ist, mit der UEM interagiert.
- Zur Verwendung dieser Funktion müssen Gerätebenutzer folgende Anforderungen erfüllen:
  - Benutzer müssen unter Entra ID vorhanden sein und über eine gültige Intune-Lizenz verfügen. Weitere Informationen finden Sie unter Microsoft Intune-Lizenzen.
  - Wenn Sie Ihr lokales Active Directory mit Entra ID synchronisieren, muss der lokale Active Directory-UPN der Benutzer mit deren Entra ID-UPN übereinstimmen.
  - Benutzer müssen als Verzeichnisbenutzer zu UEM hinzugefügt werden.
- Nachdem Sie überprüft haben, dass die oben genannten Voraussetzungen vorliegen, führen Sie die Schritte unter Konfigurieren des bedingten Zugriffs mit Entra ID aus.
  - Beachten Sie, dass Sie in den Konfigurationsschritten aufgefordert werden, den UEM Client für die Registrierung in BlackBerry Dynamics zu aktivieren und den UEM Client auf Geräten zu installieren.
  - In den Schritten werden Sie angewiesen, die Microsoft Authenticator-App vor der Aktivierung mit UEM auf den Geräten der Benutzer zu installieren. Wenn Sie die Registrierung des bedingten Zugriffs auf

dem Gerät verzögern möchten, bis die Microsoft Authenticator-App installiert ist (entweder manuell durch den Benutzer oder bereitgestellt mit UEM), können Sie die Einstellung „Start der Registrierung für bedingten Zugriff, nachdem der Authentifizierungs-Broker installiert wurde“ im zugewiesenen BlackBerry Dynamics-Profil aktivieren. Beachten Sie, dass diese Option für Android-Geräte mit der Aktivierungsart „Benutzerdatenschutz“ nicht unterstützt wird (gilt für den Android Enterprise-Benutzerdatenschutz und den Android Management-Benutzerdatenschutz). Wenn diese Option aktiviert ist, wird nach der Installation der Microsoft Authenticator-App die Registrierung für den bedingten Zugriff eingeleitet, wenn der Benutzer den UEM Client öffnet. Wenn der geschäftliche Bereich auf Android-Geräten entsperrt ist, wird der Benutzer aufgefordert, den UEM Client zu öffnen, um die Registrierung für den bedingten Zugriff zu starten.

Konfigurieren des bedingten Zugriffs mit Entra ID

Bevor Sie beginnen: Stellen Sie sicher, dass Sie die Voraussetzungen für den bedingten Entra ID-Zugriff erfüllen.

1. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > Bedingter Zugriff auf Entra ID**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen für die Konfiguration ein.
4. Klicken Sie in der Dropdown-Liste **Entra Cloud** auf die Option **GLOBAL**.
5. Geben Sie im Feld **Entra-Mandanten-ID** den Mandantennamen Ihres Unternehmens im FQDN-Format oder eine eindeutige Mandanten-ID im GUID-Format ein.
6. Klicken Sie unter **Überschreiben der Gerätezuordnung** auf **UPN** oder **E-Mail**.

   Wenn Sie UPN wählen, überprüfen Sie, ob der Entra ID-Mandant und alle zugeordneten Verzeichnisse denselben UPN-Wert für Benutzer verwenden, bevor Sie die Verbindung speichern. Nachdem Sie die Verbindung gespeichert haben, können Sie die Überschreibung der Gerätezuordnung nicht mehr ändern.
7. Wählen Sie in der Liste **Verfügbare Unternehmensverzeichnisse** die entsprechenden Unternehmensverzeichnisse aus, und fügen Sie sie hinzu.
8. Klicken Sie auf **Speichern**.
9. Wählen Sie das Administratorkonto aus, mit dem Sie sich beim Entra-Mandanten Ihres Unternehmens anmelden möchten.
10. Akzeptieren Sie die Microsoft-Berechtigungsanforderung.
11. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Richtlinie > BlackBerry Dynamics**. Führen Sie für jedes BlackBerry Dynamics-Profil, das Sie Gerätebenutzern zuweisen möchten (z. B. das Standardprofil und alle benutzerdefinierten Profile), die folgenden Schritte aus.
    a) Öffnen und bearbeiten Sie das Profil.
    b) Wählen Sie **Anmeldung des UEM Client bei BlackBerry Dynamics aktivieren**.
    c) Wenn Sie den Registrierungsprozess für den bedingten Zugriff verzögern möchten, bis die Microsoft Authenticator-App auf Geräten installiert ist, wählen Sie **Start der Registrierung für bedingten Zugriff, nachdem der Authentifizierungs-Broker installiert wurde**.
    d) Klicken Sie auf **Speichern**.
    e) Weisen Sie das Profil ggf. Benutzern und Gruppen zu.
12. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Netzwerke und Verbindungen > BlackBerry Dynamics-Konnektivität**. Führen Sie für jedes BlackBerry Dynamics-Konnektivitätsprofil, das Sie Gerätebenutzern zuweisen möchten (z. B. das Standardprofil und alle benutzerdefinierten Profile), die folgenden Schritte aus.
    a) Öffnen und bearbeiten Sie das Profil.
    b) Klicken Sie im Abschnitt **App-Server** auf **Hinzufügen**.
    c) Suchen und wählen Sie **Funktion – Azure Conditional Access** aus.

d) Klicken Sie auf **Speichern**.
e) Klicken Sie in der Tabelle **Azure Conditional Access** auf +.
f) Geben Sie in das Feld **Server** `gdas-<UEM_SRP_ID>.<region_code>.bbsecure.com` ein.
g) Geben Sie in das Feld **Port** 443 ein.
h) Klicken Sie unter **Routingtyp** auf **Direkt**.
i) Klicken Sie auf **Speichern**.
j) Weisen Sie das Profil ggf. Benutzern und Gruppen zu.

13. Weisen Sie die App **Feature – Azure Conditional Access** Benutzern oder Gruppen zu. Weitere Informationen finden Sie unter Benutzerkonten verwalten und Benutzergruppe verwalten.
14. Erstellen und konfigurieren Sie ein Konformitätsprofil und weisen Sie das Profil bei Bedarf Benutzern und Gruppen zu. Die folgende Tabelle zeigt, wie UEM-Konformitätsaktionen an Intune gemeldet werden:

Erzwingungsaktion von UEM für Konformität	Verhalten
Erzwingungsaktion: Überwachen und protokollieren	Es wird nichts an Intune gemeldet.
Erzwingungsaktion: • Nicht vertrauen • Nur geschäftliche Daten löschen • Alle Daten löschen	UEM benachrichtigt Entra ID, wenn alle Benutzeraufforderungen abgelaufen sind.
Erzwingungsaktion für BlackBerry Dynamics-Apps: Überwachen und protokollieren	Es wird nichts an Intune gemeldet.
Erzwingungsaktion für BlackBerry Dynamics: • Ausführen von BlackBerry Dynamics-Apps nicht zulassen • BlackBerry Dynamics-Appdaten löschen	UEM benachrichtigt, Entra ID, sobald der Konformitätsverstoß erkannt wird.

15. Installieren Sie sowohl die UEM Client- als auch die Microsoft Authenticator-App auf den Geräten der Benutzer. Sie können die Microsoft Authenticator-App mit UEM zuweisen und bereitstellen (siehe Hinzufügen öffentlicher Apps zur App-Liste), oder Sie können Benutzer anweisen, sie selbst herunterzuladen.
16. Je nach E-Mail-Client, den Ihr Unternehmen verwenden möchte, müssen Sie zusätzliche Schritte durchführen, um sicherzustellen, dass der E-Mail-Client mit Entra validieren und kommunizieren kann:
    - Für BlackBerry Work, siehe Konfigurieren der BlackBerry Work-App-Konfiguration für den bedingten Entra ID-Zugriff im BlackBerry Work-Administrationshandbuch.
    - Informationen zum nativen E-Mail-Client von iOS finden Sie in KB 94163.
    - Android Gmail finden Sie in KB 94494.

Wenn Sie fertig sind:

- Wenn ein Benutzer sein Gerät aktiviert, fordert ihn der UEM Client auf, sich mit bedingtem Zugriff mit Entra zu registrieren. Benutzer mit aktivierten Geräten werden beim nächsten Öffnen des UEM Client aufgefordert, sich für den bedingten Zugriff mit Entra zu registrieren.
  Hinweis: Weisen Sie die Benutzer an, die Registrierung mit Entra zu initiieren, indem sie den UEM Client verwenden, ohne dass Anmeldeoptionen innerhalb von Microsoft Authenticator verwendet werden. Die Registrierungsaufforderung des UEM Client öffnet Microsoft Authenticator, um den Benutzer zur Eingabe der Anmeldeinformationen und zum Abschluss des Registrierungsprozesses aufzufordern.
- Nachdem ein Benutzer ein Gerät mit UEM aktiviert hat, können Sie die Geräteeigenschaften des Benutzers in Microsoft Endpoint Manager überprüfen, um zu bestätigen, dass es wie erwartet bei Entra registriert wurde.

Der Name des Geräts hat folgendes Format: <*username*> - <*platform*> Unbekannt Unbekannt - <*xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx*>.

- Wenn Sie den Umfang von Benutzern oder Gruppen in der Entra-Partnerkonformitäts-Konfiguration ändern, navigieren Sie im Entra-Portal zu den Sicherheitsberechtigungen für BlackBerry UEM Conditional Access und erteilen Sie erneut die Zustimmung des Administrators für BlackBerry.
- Wenn Sie ein Gerät von UEM entfernen, bleibt das Gerät für den bedingten Zugriff mit Entra ID registriert. Benutzer können ihr Entra ID-Konto aus den Kontoeinstellungen in der Microsoft Authenticator-App entfernen, oder Sie können das Gerät aus dem Entra-Portal entfernen.

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 -macOSGeräten verwenden möchten. Wenn Sie mehr als eine 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.

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 die Apple-ID in der Verwaltungskonsole notieren. Sie können zudem 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 UEM keine Daten mehr. Wenn Sie ein neues APNs-Zertifikat registrieren, müssen Benutzer ihre Geräte neu aktivieren, um Daten zu empfangen.

Es hat sich bewährt, auf die Verwaltungskonsole und das Apple Push Certificates Portal über Google Chrome oder Safari zuzugreifen, da diese Browser optimale Unterstützung für die Anforderung und Registrierung von APNs-Zertifikaten bieten.

Anfordern und Registrieren eines APNs-Zertifikats

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie im Abschnitt **Schritt 1 von 3 – Signiertes CSR-Zertifikat von BlackBerry herunterladen** auf **Zertifikat herunterladen**.
3. Speichern Sie die signierte CSR-Datei auf Ihrem Computer.
4. Klicken Sie im Abschnitt **Schritt 2 von 3 – APNs-Zertifikat von Apple anfordern** auf **Apple Push Certificates Portal**.
5. Melden Sie sich beim Apple Push Certificates Portal mit einer gültigen Apple-ID an.
6. Befolgen Sie die Anweisungen zum Hochladen der signierten CSR-Datei.

   Wenn eine Fehlermeldung über einen ungültigen Dateityp angezeigt wird, können Sie die Datei in eine .txt-Datei umbenennen und erneut hochladen.
7. Laden Sie das APNs-Zertifikat auf Ihren Computer herunter, und speichern Sie es.
8. Klicken Sie in der Verwaltungskonsole im Abschnitt **Schritt 3 von 3 – APNs-Zertifikat registrieren** auf **Durchsuchen**.
9. Navigieren Sie zu dem APNs-Zertifikat, und wählen Sie es aus.
10. Klicken Sie auf **Submit**.

Wenn Sie fertig sind:

- Klicken Sie zum Testen der Verbindung zwischen UEM und dem APNs-Server auf **APNs-Zertifikat testen**.
- Das APNs-Zertifikat ist ein Jahr lang gültig. Sie müssen das APNs-Zertifikat jedes Jahr vor dem Ablaufdatum erneuern. Verwenden Sie hierzu die Apple-ID, die Sie zum Abrufen des originalen APNs-Zertifikats verwendet haben. Um das Zertifikat zu erneuern, wiederholen Sie die oben beschriebenen Schritte, aber klicken Sie in Schritt 2 auf **Zertifikat erneuern**.

Fehlerbehebung: APNs

Problem	Mögliche Lösung
Beim Versuch, eine signierte CSR abzurufen, erhalten Sie folgende Fehlermeldung: „Im System ist ein Fehler aufgetreten. Versuchen Sie es erneut.“	Siehe KB 37266.
Wenn Sie versuchen, das APNs-Zertifikat zu registrieren, erhalten Sie die Fehlermeldung „Das APNs-Zertifikat stimmt nicht mit dem CSR überein“.	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.
Sie können iOS- oder macOS-Geräte nicht aktivieren.	Das APNs-Zertifikat ist möglicherweise nicht richtig registriert. Überprüfen Sie Folgendes: • 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 können BlackBerry UEM so konfigurieren, dass es mit dem Programm zur Geräteregistrierung (DEP) von Apple synchronisiert wird, wenn Sie die UEM-Verwaltungskonsole zur Verwaltung der Aktivierung der iOS-Geräte verwenden möchten, die Ihr Unternehmen für DEP erworben hat.

1. Navigieren Sie in der Verwaltungskonsole zu **Einstellungen > Externe Integration > Programm zur Geräteregistrierung von Apple**.

   Wenn Sie UEM lokal verwenden, klicken Sie auf +, und geben Sie einen Namen für das Konto ein.
2. Klicken Sie in Abschnitt **1 von 4: Erstellen eines Apple DEP-Kontos** auf **Erstellen eines Apple DEP-Kontos**.
3. Füllen Sie die Felder aus, und befolgen Sie die Anweisungen zum Erstellen des Kontos.
4. Klicken Sie in Abschnitt **2 von 4: Herunterladen eines öffentlichen Schlüssels** auf **Herunterladen des öffentlichen Schlüssels**.
5. Speichern Sie den öffentlichen Schlüssel auf Ihrem lokalen Computer.
6. Klicken Sie in Abschnitt **3 von 4: Erzeugen eines Server-Tokens aus dem Apple DEP-Konto** auf **Öffnen des DEP-Portals von Apple**.
7. Melden Sie sich bei Ihrem DEP-Konto an. Laden Sie in den Einstellungen für Ihr Konto das Server-Token für den MDM-Server herunter.
8. Klicken Sie in Abschnitt **4 von 4: Registrieren des Server-Tokens bei BlackBerry UEM** auf **Durchsuchen**.
9. Navigieren Sie zur Server-Token-Datei mit der Erweiterung .p7m, und wählen Sie sie aus. Klicken Sie auf **Öffnen** und dann auf **Weiter**.
10. Geben Sie im Fenster der Registrierungskonfiguration einen Namen für die Konfiguration ein.
11. Wenn UEM die Registrierungskonfiguration automatisch Geräten zuweisen soll, sobald Sie sie in Apple DEP registrieren, aktivieren Sie das Kontrollkästchen **Alle neuen Geräte automatisch dieser Konfiguration zuweisen**. Wählen Sie diese Option nicht aus, wenn Sie die UEM-Verwaltungskonsole verwenden möchten, um die Registrierungskonfiguration manuell bestimmten Geräten zuzuweisen.
12. Geben Sie optional einen Abteilungsnamen und eine Supporttelefonnummer ein, die während der Einrichtung auf Geräten angezeigt werden sollen.
13. Wählen Sie im Abschnitt **Gerätekonfiguration** eine der folgenden Optionen:
    - **Kopplung zulassen**: Benutzer können das Gerät mit einem Computer koppeln.
    - **Erforderlich**: Benutzer können Geräte mit ihrem Unternehmensbenutzernamen und -kennwort aktivieren.
    - **Entfernen des MDM-Profils zulassen**: Benutzer können Geräte deaktivieren.
    - **Warten, bis das Gerät konfiguriert wurde**: Benutzer können die Geräteeinrichtung nicht abbrechen, bevor die Aktivierung in UEM abgeschlossen wurde.
14. Wählen Sie im Abschnitt **Bei der Einrichtung überspringen** die Elemente aus, die nicht in der Geräteeinrichtung enthalten sein sollen:

Option	Auswirkungen bei Auswahl
Kennung	Benutzer werden nicht aufgefordert, eine Gerätekennung zu erstellen.
Standortdienste	Standortdienste sind auf dem Gerät deaktiviert.
Wiederherstellen	Benutzer können keine Daten aus einer Sicherungsdatei wiederherstellen.
Verschieben von Android	Daten können von einem Android-Gerät nicht wiederhergestellt werden.

Option	Auswirkungen bei Auswahl
Apple-ID	Benutzer können sich nicht bei Apple-ID und iCloud anmelden.
Geschäftsbedingungen	Benutzer sehen die Geschäftsbedingungen von iOS nicht.
Siri	Siri ist auf Geräten deaktiviert.
Diagnostics	Diagnoseinformationen werden während der Einrichtung nicht automatisch vom Gerät gesendet.
Biometrisch	Benutzer können Touch ID nicht einrichten.
Zahlung	Benutzer können Apple Pay nicht einrichten.
Zoom	Benutzer können Zoom nicht einrichten.
Home-Taste einrichten	Benutzer können den Klick auf die Home-Taste nicht anpassen.
Bildschirmzeit	Die Option zum Einrichten der Bildschirmzeit wird während der DEP-Registrierung übersprungen.
Softwareupdate	Benutzern wird der Bildschirm für obligatorische Softwareupdates auf dem Gerät nicht angezeigt.
iMessage und FaceTime	Benutzer sehen den Bildschirm für iMessage und FaceTime auf dem Gerät nicht.
Anzeigename	Benutzern wird der Bildschirm für den Anzeigenamen auf dem Gerät nicht angezeigt.
Datenschutz	Benutzern wird der Bildschirm für den Datenschutz auf dem Gerät nicht angezeigt.
Onboarding	Benutzern wird der Informationsbildschirm für das Onboarding auf dem Gerät nicht angezeigt.
Watch-Migration	Benutzern wird der Informationsbildschirm für die Watch-Migration auf dem Gerät nicht angezeigt.
SIM-Setup	Benutzern wird der Bildschirm für das Einrichten eines Mobilfunkvertrags auf dem Gerät nicht angezeigt.
Migration von Gerät zu Gerät	Benutzern wird der Informationsbildschirm für die Migration von Gerät zu Gerät auf dem Gerät nicht angezeigt.

15. Klicken Sie auf **Speichern**. 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 zum Aktivieren von beim DEP registrierten Geräten finden Sie unter Aktivieren von beim DEP registrierten iOS-Geräten.

- 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. Um das Token zu erneuern, klicken Sie unter **Einstellungen > Externe Integration > Programm zur Geräteregistrierung von Apple** auf das DEP-Konto und dann auf **Server-Token aktualisieren**. Führen Sie beide Schritte aus, um ein neues Server-Token zu generieren und bei UEM zu registrieren.
- Sie können jede von Ihnen erstellte DEP-Verbindung entfernen. Wenn Sie alle DEP-Verbindungen entfernen, können Sie keine neuen Apple-DEP-Geräte aktivieren. Wenn Sie Geräten Registrierungskonfigurationen zuweisen und die Konfigurationen nicht angewendet wurden, entfernt UEM die Registrierungskonfigurationen, die den Geräten zugewiesen sind. Das Entfernen der Verbindung wirkt sich nicht auf Geräte aus, die auf UEM aktiviert sind.

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. In der folgenden Tabelle werden die unterschiedlichen Optionen für die Konfiguration von BlackBerry UEM zur Unterstützung von Android Enterprise-Geräten zusammengefasst:

Methode	Wann diese Methode verwendet werden sollte	Typ des Benutzerkontos	Unterstützte Google-Dienste
Verbinden einer UEM-Domäne mit einer Google Workspace-Domäne.	Ihr Unternehmen verwendet eine Google Workspace-Domäne.	Google Workspace-Konten (für Unternehmen)	• Alle Google Workspace-Dienste wieGmail, Google Calendar und Drive • App-Verwaltung durch Google Play
Verbinden einer UEM-Domäne mit einer Google Cloud-Domäne.	Ihr Unternehmen verwendet eine Google Cloud-Domäne.	Google Cloud-Konten, die auch als Managed Google-Konten (für Unternehmen) bezeichnet werden	• Ähnlich wie Google Workspace, aber ohne Zugriff auf kostenpflichtige Produkte, z. B. Gmail, Google Calendar und Drive • App-Verwaltung durch Google Play
Zulassen, dass UEMAndroid Enterprise-Geräte verwaltet, die über verwaltete Google Play-Konten verfügen.	Ihr Unternehmen verwendet keine Google- oder Google-Domäne, die bereits mit einer UEM-Domäne verbunden ist, und Sie möchten Android Enterprise-Geräte in einer zweiten UEM-Domäne nutzen.	Android Enterprise-Geräte mit verwalteten Google Play-Konten	• App-Verwaltung durch Google Play • Google-Dienste werden nicht unterstützt

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

Bevor Sie beginnen: Wenn Sie zuvor eine UEM-Domäne mit einer Google-Domäne verbunden haben und eine neue UEM-Domäne verbinden möchten, müssen Sie die vorhandene Verbindung entfernen. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Google-Domänenverbindung**, und entfernen Sie die Verbindung. Sie können die Verbindung auch über die Admin-Einstellungen in Google Play (https://play.google.com/work) entfernen, indem Sie dasselbe Google-Konto verwenden, das Sie zum Erstellen der Verbindung verwendet haben. Wenn Sie eine Verbindung entfernen, deaktivieren Sie damit auch alle Geräte, die mit einer Android Enterprise-Aktivierungsart aktiviert wurden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Verwaltung von Android und Chrome**.
2. Führen Sie einen der folgenden Schritte 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-, einem Google oder einem Gmail-Konto an. 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**.
Verwenden einer Google-Domäne.	**a.** Wählen Sie **Verbinden Sie BlackBerry UEM mit Ihrer vorhandenen Google-Domäne**. Beachten Sie, dass Sie keine Google-Domänen zwischen mehreren UEM-Domänen freigeben können. Diese Option unterstützt Android Enterprise und Chrome OS Enterprise. **b.** Klicken Sie auf **Weiter**. **c.** Füllen Sie die Felder zum Erstellen eines Dienstkontos aus, und klicken Sie auf **Weiter**.

3. Führen Sie einen der folgenden Schritte aus:
   - Um App-Konfigurationsdetails über die BlackBerry Infrastructure zu senden, wählen Sie **App-Konfiguration über UEM Client senden**.
   - Um App-Konfigurationsdetails über die Google-Infrastruktur zu senden, wählen Sie **App-Konfiguration mit Google Play senden**.
4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Annehmen**, um die Berechtigungen für einige oder alle der angezeigten Google- und BlackBerry-Apps zu akzeptieren.
5. Klicken Sie auf **Fertig**.

Wenn Sie fertig sind:

- Schließen Sie die Schritte für die Aktivierung von Android Enterprise-Geräten ab. Weitere Informationen zur Geräteaktivierung finden Sie unter Aktivieren von Android-Geräten in der Dokumentation für Administratoren.
- Sie können die Google-Domänenverbindung über Einstellungen > Externe Integration bearbeiten, um den Typ der Google-Domäne zu ändern, den Sie verwenden, oder um die Domänenverbindung zu testen.
- Wenn Sie eine UEM-Domäne, die mit Google verbunden ist, außer Betrieb nehmen möchten, entfernen Sie die Verbindung, bevor Sie die Domäne deaktivieren (Einstellungen > Externe Integration > Google-Domänenverbindung). Sie können die Verbindung auch über die Admin-Einstellungen in Google Play (https://play.google.com/work) entfernen, indem Sie dasselbe Google-Konto verwenden, das Sie zum Erstellen der Verbindung verwendet haben. Wenn Sie eine Verbindung entfernen, deaktivieren Sie damit auch alle Geräte, die mit einer Android Enterprise-Aktivierungsart aktiviert wurden.

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

Android Management-Geräte bieten zusätzliche Sicherheit für Unternehmen, die ihre Geräte mit der Android Management-API verwalten möchten.

Bevor Sie Geräte mit Android Management-Aktivierungsarten aktivieren, lesen Sie die Überlegungen zu Aktivierungsarten für Android Management.

Schritt	Aktion
1	Konfigurieren von Android Management in der Google Cloud-Konsole.
2	Konfigurieren von Android Management in BlackBerry UEM.

Konfigurieren von Android Management in der Google Cloud-Konsole

Sie müssen Android Enterprise mit einem verwalteten Google Play-Konto einrichten, bevor Sie auf die Option zur Konfiguration von Android Management zugreifen können.

Bei der Einrichtung von Android Management müssen Sie eine dedizierte E-Mail-Adresse verwenden. Sie dürfen nicht dieselbe E-Mail-Adresse verwenden, die Sie zur Einrichtung von Android Enterprise verwendet haben.

1. Gehen Sie zu https://console.developers.google.com, und melden Sie sich mit der E-Mail-Adresse an, die für Android Management verwendet wird.
2. Klicken Sie in der Cloud-Konsole auf **Neues Projekt**.
3. Klicken Sie auf **APIs und Dienste > Bibliothek auswählen**.
4. Suchen Sie im Suchfeld nach der Android Management-API.
5. Aktivieren Sie in der Liste der Suchergebnisse **Android Management API** und **Cloud Pub/Sub API**.
6. Klicken Sie in der Menüleiste der Cloud-Konsole auf **IAM & Admin > Dienstkonten > Auswählen > Dienstkonto erstellen**.
7. Wählen Sie im Abschnitt **Diesem Dienstkonto Zugriff auf das Projekt gewähren** in der Dropdown-Liste **Rolle** die Option **Android Management-Benutzer** aus.
8. Wählen Sie in der zweiten Dropdown-Liste **Rolle** die Option **Pub/Sub Admin** aus.
9. Geben Sie im Abschnitt **Benutzern Zugriff auf das Dienstkonto gewähren** die E-Mail-Adresse ein, die Sie in Schritt 1 verwendet haben.
10. Klicken Sie auf **Fertig**.
11. Klicken Sie in der Menüleiste auf **Dienstkonten**, und wählen Sie das erstellte Konto aus.
12. Klicken Sie auf **Schlüssel > Schlüssel hinzufügen**.
13. Wählen Sie im Dialogfeld **Privaten Schlüssel für „*<service_account_name>*“ erstellen JSON**. Klicken Sie auf **Erstellen**.
14. Notieren Sie den Namen des Dienstkontos, die E-Mail-Adresse des Administrators des Dienstkontos und den privaten JSON-Schlüssel.

Wenn Sie fertig sind: Konfigurieren von Android Management in BlackBerry UEM.

Konfigurieren von Android Management in BlackBerry UEM

Bevor Sie beginnen:

- Konfigurieren von Android Management in der Google Cloud-Konsole.
- Stellen Sie sicher, dass Android Enterprise bereits in UEM konfiguriert wurde. Siehe Konfigurieren von BlackBerry UEM für die Unterstützung von Android Enterprise-Geräten.
- Stellen Sie sicher, dass Sie über den Namen des Android Management-Dienstkontos, die E-Mail-Adresse des Administrators des Dienstkontos und den privaten JSON-Schlüssel verfügen.

1. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > Verwaltung von Android und Chrome**.
2. Klicken Sie auf **Hinzufügen einer Android Management-Verbindung**.
3. Geben Sie im Feld **Anzeigename des Unternehmens** den Namen des Dienstkontos ein.
4. Geben Sie im Feld **E-Mail-Adresse des Administrators** die E-Mail-Adresse des Dienstkontos ein.
5. Geben Sie im Feld **Info zum Dienstkonto (json-Format)** den privaten JSON-Schlüssel ein.
6. Klicken Sie auf **Speichern**.
7. Geben Sie im Dialogfeld **Domänenname oder Geschäftsname** im Feld **Ihre Antwort** den Namen des Android Management-Dienstkontos ein. Klicken Sie auf **Weiter**.

Erweiterung der Verwaltung von Chrome OS-Geräten auf BlackBerry UEM

Sie können BlackBerry UEM mit einer verwalteten Google-Domäne integrieren, um einige Chrome OS-Verwaltungsfunktionen auf UEM zu erweitern. Die Google-Domäne muss das Chrome Enterprise-Upgrade enthalten. Beachten Sie, dass die Registrierung und Verwaltung von Chrome OS-Geräten weiterhin über die verwaltete Google-Domänenkonsole erfolgt.

UEM synchronisiert Organisationseinheiten aus der Google-Verwaltungskonsole und gliedert sie in UEM-Gruppen von Organisationseinheiten. Nach der ersten Synchronisierung registriert sich UEM bei der Google-Domäne, um über Änderungen an Organisationseinheiten, Benutzern oder Geräten benachrichtigt zu werden. Wenn UEM über eine Änderung benachrichtigt wird, wird die Datenbank entsprechend synchronisiert und aktualisiert.

Schritt	Aktion
1	Erstellen eines Dienstkontos zur Authentifizierung bei der Google-Domäne.
2	Aktivieren von UEM zur Synchronisierung der Chrome OS-Daten.
3	Integration von UEM in die Google-Domäne.

Wenn Sie UEM bereits zur Unterstützung von Android Enterprise-Geräten konfiguriert haben, können Sie die folgenden Schritte ausführen, um zuzulassen, dass UEM Chrome OS-Geräte verwaltet:

Schritt	Aktion
1	Stellen Sie sicher, dass die Google Ihres Unternehmens für Chrome OS Enterprise aktiviert ist.
2	Stellen Sie sicher, dass die Chrome-Richtlinien-API in der Google-Domäne Ihres Unternehmens aktiviert ist. Weitere Informationen finden Sie unter Erstellen eines Dienstkontos zur Authentifizierung bei der Google-Domäne.
3	Stellen Sie sicher, dass alle Geltungsbereiche hinzugefügt wurden. Weitere Informationen finden Sie unter Aktivieren von UEM zur Synchronisierung der Chrome OS-Daten.
4	Aktivieren Sie die Chrome OS-Verwaltung in der UEM-Konsole. Weitere Informationen finden Sie unter Integration von UEM in die Google-Domäne.

Erstellen eines Dienstkontos zur Authentifizierung bei der Google-Domäne

Führen Sie diese Schritte nur aus, wenn BlackBerry UEM noch nicht mit einer vorhandenen verwalteten Google-Domäne verbunden ist.

1. Melden Sie sich mit dem Google-Konto, das Sie für die Verwaltung Ihres Projekts verwenden möchten, bei der Google Developers-Konsole an.
2. Erstellen ein Projekt.
3. Wählen Sie das Projekt aus, und erstellen Sie ein Dienstkonto für das Projekt.
4. Geben Sie dem Dienstkonto die Rolle **Basis > Editor**.
5. Wählen Sie das Dienstkonto aus, und fügen Sie einen neuen P12-Schlüssel hinzu.
6. Kopieren Sie das Kennwort für den privaten Schlüssel, und speichern Sie das Zertifikat auf Ihrem lokalen Computer.
7. Kopieren Sie die eindeutige Client-ID und E-Mail-Adresse für das Dienstkonto.
8. Suchen Sie im Abschnitt für aktivierte APIs und Dienste nach den folgenden APIs, und aktivieren Sie sie:
   - **Admin SDK API**
   - **Google Play EMM API**
   - **Chrome Policy API**

Wenn Sie fertig sind: Aktivieren von UEM zur Synchronisierung der Chrome OS-Daten.

Aktivieren von UEM zur Synchronisierung der Chrome OS-Daten

Sie müssen die Google-Verwaltungskonsole Ihres Unternehmens verwenden, um zusätzliche APIs zu aktivieren, damit UEM Chrome OS Daten synchronisieren kann.

Bevor Sie beginnen: Erstellen eines Dienstkontos zur Authentifizierung bei der Google-Domäne.

1. Melden Sie sich mit dem Administratorkonto für Ihre Google-Domäne bei der Google-Verwaltungskonsole an.
2. Navigieren Sie zum Abschnitt für Integrationen von Drittanbietern für Mobilgeräte.
3. Stellen Sie sicher, dass die Android-Mobilverwaltung von Drittanbietern aktiviert ist.
4. Generieren Sie im Abschnitt zum Hinzufügen von EMM-Anbietern ein Token.
5. Kopieren Sie das Token.
6. Klicken Sie im Abschnitt zu Sicherheits-API-Kontrollen auf die Option zum Verwalten der domänenweiten Delegierung.
7. Fügen Sie eine neue Konfiguration hinzu.
8. Fügen Sie als Client-ID die eindeutige Client-ID für das Google-Dienstkonto ein.
9. Geben Sie für OAuth-Bereiche Folgendes ein, oder fügen Sie es in eine durch Komma getrennte Liste ein:
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.customer
   - https://www.googleapis.com/auth/admin.directory.device.chromeos
   - https://www.googleapis.com/auth/admin.directory.device.mobile
   - https://www.googleapis.com/auth/admin.directory.orgunit
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/chrome.management.policy
   - https://www.googleapis.com/auth/admin.reports.audit.readonly
10. Autorisieren Sie die Verbindung.

Wenn Sie fertig sind: Integration von UEM in die Google-Domäne.

Integration von UEM in die Google-Domäne

Bevor Sie beginnen: Aktivieren von UEM zur Synchronisierung der Chrome OS-Daten.

1. Melden Sie sich mit einem Sicherheitsadministrator-Konto bei der Verwaltungskonsole von UEM an.
2. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Verwaltung von Android und Chrome**.
3. Wählen Sie **Verbinden Sie BlackBerry UEM mit Ihrer vorhandenen Google-Domäne**.
4. Wählen Sie unter **Wie App-Konfigurationen gesendet werden** die Option **App-Konfiguration mit Google Play senden** aus.
5. Klicken Sie auf **Weiter**.
6. Fügen Sie im Feld **Kennwort des privaten Schlüssels** das Kennwort aus der Google Developers-Konsole ein.
7. Klicken Sie auf **Durchsuchen**.
8. Navigieren Sie zur Zertifikatsdatei aus der Google Developers-Konsole, und wählen Sie sie aus.
9. Fügen Sie im Feld **E-Mail-Adresse des Dienstkontos** die E-Mail-Adresse des Google-Dienstkontos aus der Google Developers-Konsole ein.
10. Geben Sie im Feld **E-Mail-Adresse des Google-Administrators** die E-Mail-Adresse des Administratorkontos ein, das für die Verwaltung von Google Cloud oder Google Workspace, je nach Google-Domäne, verwendet wird.
11. Fügen Sie im Feld **Token** das Token ein, das Sie generiert haben.
12. Wählen Sie im Abschnitt **Typ der Domäne zur Verwaltung von Android-Geräten mit einem geschäftlichen Profil auswählen** die entsprechende Google-Domäne aus.
13. Wenn Sie **Google Cloud-Domäne** ausgewählt haben, wählen Sie eine der folgenden Optionen aus:
    - **Nicht zulassen, dass BlackBerry UEM Benutzer in der Domäne erstellt**: Wenn Sie diese Option auswählen, müssen Sie Benutzer in Ihrer Google Cloud-Domäne und lokale Benutzer mit denselben E-Mail-Adressen in UEM erstellen.
    - **Zulassen, dass BlackBerry UEM Benutzer in der Domäne erstellt**: Wenn Sie diese Option aktivieren, wählen Sie eine der folgenden Optionen aus:
      - **Nicht zulassen, dass BlackBerry UEM Benutzer in der Google-Domäne löscht**
      - **Zulassen, dass BlackBerry UEM Benutzer in der Google-Domäne löscht**
14. Klicken Sie auf **Weiter** und wählen Sie aus, welche Anwendungen Sie zu UEM hinzufügen möchten.
15. Klicken Sie auf **Weiter**.
16. Klicken Sie erneut auf **Weiter**.

Wenn Sie fertig sind: Um UEM mit der Google-Verwaltungskonsole zu synchronisieren, klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Verwaltung von Android und Chrome**. Klicken Sie im Abschnitt **Chrome OS-Verwaltung** auf **Aktivieren**. UEM führt eine erste Datensynchronisierung innerhalb von zehn Minuten durch und plant regelmäßige Synchronisierungen. Nachdem die Synchronisierung abgeschlossen ist, können Sie über die Optionen auf diesem Bildschirm Synchronisierungen für Organisationseinheiten, Benutzer und Geräte außerhalb des Zeitplans initiieren.

Vereinfachung von Windows 10-Aktivierungen

Wenn ein Benutzer ein Windows 10-Gerät mit BlackBerry UEM aktiviert, muss der Benutzer die UEM-Serveradresse angeben. Sie können den Aktivierungsprozess für Benutzer mit den folgenden Methoden vereinfachen:

Methode	Beschreibung
Integrieren von UEM mit Entra ID-Einbindung.	Wenn Sie die Entra ID-Einbindung konfigurieren, können Benutzer Ihre Gerät nur mit Ihrem Entra ID-Benutzernamen und -Kennwort aktivieren. Es ist eine Entra ID-Premium-Lizenz erforderlich. Siehe Integrieren von UEM mit Entra ID-Einbindung.
Konfigurieren Sie Windows Autopilot.	Wenn Sie Windows Autopilot konfigurieren, ist die Registrierung Teil der vorkonfigurierten Einrichtungserfahrung, und das Gerät wird automatisch aktiviert, wenn der Benutzer sie nur mit seinem Entra ID-Benutzernamen und -Kennwort abschließt. Integration mit Entra ID-Einbindung und eine Entra ID-Premium-Lizenz sind erforderlich. Siehe Konfigurieren von Windows Autopilot für die Geräteaktivierung.
Bereitstellen eines Suchdienstes.	Sie können eine Java-Webanwendung von BlackBerry als Suchdienst verwenden. Sie können verschiedene Betriebssysteme und Webanwendungs-Tools zur Bereitstellung einer Suchdienst-Webanwendung verwenden. Siehe Bereitstellen eines Suchdienstes zur Vereinfachung von Windows 10-Aktivierungen.

Integrieren von UEM mit Entra ID-Einbindung

Sie können BlackBerry UEM mit Entra ID-Einbindung integrieren, um den Registrierungsprozess für Windows 10-Geräte zu vereinfachen. Nach der Konfiguration können Benutzer ihre Geräte mit UEM unter Zuhilfenahme ihres Entra ID-Benutzernamens und -Kennworts registrieren. Entra ID-Einbindung ist auch für die Unterstützung von Windows Autopilot erforderlich, wodurch Windows 10-Geräte während der vorkonfigurierten Windows 10-Einrichtung automatisch mit UEM aktiviert werden. Ein UEM-Zertifikat kann manuell auf dem Gerät installiert werden, oder Administratoren können das Zertifikat mithilfe von SCCM bereitstellen.

Bevor Sie beginnen: Sie benötigen die URL für MDM-Nutzungsbedingungen, die MDM-Such-URL und die App-ID-URI, um die folgenden Schritte auszuführen. Um diese URLs zu bestimmen, erstellen Sie in der UEM-Verwaltungskonsole ein Testbenutzerkonto, und senden Sie dem Benutzer eine Aktivierungs-E-Mail mit der Standard-E-Mail-Vorlage für Aktivierungen. Die Standardvorlage enthält die Variable %ClientlessActivationURL%, die in der empfangenen E-Mail auf den entsprechenden Wert aufgelöst wird. Verwenden Sie diesen Wert für die folgenden URLs in den folgenden Schritten:

- URL für MDM-Nutzungsbedingungen: *%ClientlessActivationURL%*/azure/termsofuse
- MDM-Such-URL: *%ClientlessActivationURL%*/azure/discovery
- App-ID-URI: *%ClientlessActivationURL%*

1. Melden Sie sich beim Microsoft Entra ID-Verwaltungsportal an.
2. Fügen Sie im Abschnitt zur Verwaltung von MDM und MAM eine lokale MDM-Anwendung hinzu, und geben Sie ihr einen Anzeigenamen (z. B. `BlackBerry UEM`).
3. Klicken Sie auf die Anwendung, die Sie zur Konfiguration ihrer Einstellungen hinzugefügt haben.

4. Geben Sie den Benutzerbereich an. Wählen Sie ggf. Gruppen aus.
5. Geben Sie die URL für die MDM-Nutzungsbedingungen und die MDM-Such-URL an.
6. Speichern Sie die Änderungen.
7. Geben Sie in den Eigenschaften für die Einstellungen der lokalen MDM-Anwendung die App-ID-URI an.
8. Speichern Sie.

Wenn Sie fertig sind: Optional Konfigurieren von Windows Autopilot für die Geräteaktivierung.

Konfigurieren von Windows Autopilot für die Geräteaktivierung

Wenn Sie Windows Autopilot konfigurieren, wird das Gerät automatisch aktiviert, wenn der Benutzer die vorkonfigurierte Einrichtung nur mit seinem Entra ID-Benutzernamen und -Kennwort abschließt.

Bevor Sie beginnen: Integrieren von UEM mit Entra ID-Einbindung.

1. Melden Sie sich beim Microsoft Entra ID-Verwaltungsportal an.
2. Erstellen Sie im Abschnitt Windows-Geräteregistrierung ein Windows Autopilot-Bereitstellungsprofil.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Konfigurieren Sie die vorkonfigurierte Einrichtung.
5. Weisen Sie den entsprechenden Benutzergruppen das Profil zu.
6. Speichern Sie das Profil.
7. Führen Sie die folgenden Schritte auf jedem Windows 10-Gerät aus, das Sie mit Windows Autopilot aktivieren möchten:
   a) Schalten Sie das Gerät ein, um die vorkonfigurierte Einrichtung zu laden, und verbinden Sie sich mit einem Wi-Fi-Netzwerk.
   b) Drücken Sie STRG + UMSCHALT + F3, um neu zu starten und in den Überwachungsmodus zu wechseln.
   c) Führen Sie Windows PowerShell als Administrator aus, und führen Sie die folgenden Befehle aus:

      ```
      Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp
      ```

      ```
      Install-Script -Name Get-WindowsAutoPilotInfo
      ```

      ```
      Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv
      ```

   d) Erfassen Sie die resultierende .csv-Datei von jedem Gerät.
8. Importieren Sie im Microsoft Entra ID-Verwaltungsportal, im Abschnitt für Windows-Geräteregistrierung und Windows Autopilot-Geräte, die .csv-Datei von jedem Gerät.
9. Führen Sie im Dialogfeld Systemvorbereitungstool die folgenden Schritte aus:
   a) Wählen Sie für die Systembereinigung die Option „Out-of-Box-Experience (OOBE) für System aktivieren“ aus, und deaktivieren Sie die Option „Verallgemeinern“.
   b) Wählen Sie in den Optionen zum Herunterfahren die Option zum Neustart aus.

Bereitstellen eines Suchdienstes zur 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.

Sie können verschiedene Betriebssysteme und Webanwendungs-Tools zur Bereitstellung einer Suchdienst-Webanwendung verwenden. Die folgenden Schritte befassen sich mit den wesentlichen Aufgaben. Die spezifischen Aktionen hängen von der Umgebung Ihres Unternehmens ab.

1. Konfigurieren Sie eine statische IP-Adresse für den Computer, der den Suchdienst hostet.
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 Sie einen DNS-Host-A-Datensatz für den Namen **enterpriseenrollment.**,<*email_domain*> der auf die statische IP-Adresse verweist, die Sie konfiguriert haben.
4. Erstellen und installieren Sie ein Zertifikat, um für sichere TLS-Verbindungen zwischen Windows 10-Geräten und dem Suchdienst zu sorgen.
5. Melden Sie sich bei myAccount an, um das Tool für die automatische Proxy-Ermittlung herunterzuladen. Führen Sie die .exe-Datei aus, um eine .war-Datei zu extrahieren.
   Die Datei `W10AutoDiscovery-<version>.war` wird unter `C:\BlackBerry` extrahiert.
6. Benennen Sie `W10AutoDiscovery-<version>.war` in `ROOT.war` um. Verschieben Sie sie in das Stammverzeichnis Ihres Java-Anwendungsservers.
7. Aktualisieren Sie die wdp.properties-Datei der Suchdienst-Webanwendung, um eine Liste der SRP-IDs (UEM lokal) oder Mandanten-IDs (UEM Cloud) für Ihre UEM-Instanzen hinzuzufügen. Sie finden die IDs in myAccount.

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 einem lokalen UEM-Quellserver migrieren. In lokalen UEM-Umgebungen können Sie auch von einem eigenständigen Good Control-Server migrieren.

Schritt	Aktion
1	Lesen Sie die Migrationsvoraussetzungen sowie Best Practices und Überlegungen.
2	Herstellen einer Verbindung zu einem Quellserver.
3	Migrieren von IT-Richtlinien, Profilen und Gruppen aus einem Quellserver.
4	Migrieren von Benutzern aus einem Quellserver.
5	Migrieren von Geräten aus einem Quellserver.

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

Objekt	Voraussetzungen
Berechtigungen des Sicherheitsadministrators	Befolgen Sie die Anweisungen in diesem Abschnitt als Sicherheitsadministrator.
Unterstützte Versionen des Quellservers	Bei lokalen UEM-Systemen können Sie von den folgenden Quellservern migrieren: • UEM lokal 12.18 oder höher • Good Control (eigenständig) 5.0 oder höher Für UEM Cloud können Sie Daten nur von UEM lokal migrieren. Die lokale UEM-Quellinstanz muss eine der drei letzten Hauptversionen sein. Ältere Versionen werden bei der Migration nicht unterstützt.
BlackBerry Connectivity Node (nur UEM Cloud)	Um alle Migrationsfunktionen zu unterstützen, müssen Sie mindestens BlackBerry Connectivity Node Version 2.13 oder höher aktivieren.

Objekt	Voraussetzungen
UEM-Unternehmensverzeichnisverbindung	Konfigurieren Sie die Verbindung mit dem UEM-Zielunternehmensverzeichnis auf die gleiche Weise wie auf dem Quellserver. Die Migration funktioniert nicht, wenn die Verbindung zum Unternehmensverzeichnis nicht übereinstimmt.
Defragmentieren der Datenbanken (nur UEM lokal)	Defragmentieren Sie die Quell- und Zieldatenbanken von UEM, bevor Sie mit der Migration beginnen. Wenn Sie eine große Anzahl von Benutzern oder Geräten migrieren, sollten Sie die UEM-Zieldatenbank nach jeder Migration einer Benutzer- oder Gerätegruppe defragmentieren.
BlackBerry UEM Client	• UEM lokal: Wenn Sie die bei BlackBerry Dynamics registrierten UEM Client- und BlackBerry Dynamics-Apps migrieren möchten, muss der neueste UEM Client auf den Geräten installiert sein. • UEM Cloud: Der UEM Client muss Version 12.x oder höher sein.
BlackBerry Dynamics-Apps	• UEM lokal: Alle BlackBerry Dynamics-Apps, die Sie migrieren möchten, müssen BlackBerry Dynamics SDK-Version 7.1 oder höher verwenden. Für Migrationen von Good Control müssen Apps SDK-Version 4.0.0 oder höher verwenden. • UEM Cloud: Alle BlackBerry Dynamics-Apps, die Sie migrieren möchten, müssen BlackBerry Dynamics SDK-Version 8.0 oder höher verwenden. • BlackBerry Dynamics-Apps, die keine Migration unterstützen, werden während der Migration vom Gerät entfernt.
BlackBerry Dynamics-App-Berechtigungen	• Der UEM-Zielserver muss über die gleiche Liste mit BlackBerry Dynamics-App-Berechtigungen wie der Quellserver verfügen. • Allen migrierten Benutzerkonten muss die gleiche Liste mit BlackBerry Dynamics-App-Berechtigungen auf dem Ziel-UEM zugewiesen sein wie auf dem Quellserver. • Der Authentifikator muss auf dem Quellserver und dem Zielserver identisch sein. Sie können den Authentifikator nach der Migration ändern. • Wenn das BlackBerry Dynamics-Profil auf dem Quellserver zulässt, dass UEM Client von BlackBerry Dynamics aktiviert werden kann, konfigurieren Sie ihn auch auf dem Zielserver. • Der Authentifikator muss auf dem Quellserver und dem UEM-Zielserver identisch sein. Sie können den Authentifikator nach der Migration ändern. • Bei Migrationen von einer Good Control-Instanz werden Geräte mit einem Geräte-Authentifikator von Good for Enterprise nicht migriert. Nach dem Entfernen von Good for Enterprise als Authentifikator müssen Sie den Cache aktualisieren, bevor Sie mit der Migration fortfahren. Wenn Berechtigungen zwischen Quell- und Zielserver nicht übereinstimmen, werden BlackBerry Dynamics-Apps nach der Migration deaktiviert.

Objekt	Voraussetzungen
Benutzerdefinierte BlackBerry Dynamics-Apps	Benutzerdefinierte Apps werden nur migriert, wenn die Quell- und Zielserver dieselbe Unternehmens-ID aufweisen. Weitere Informationen über die Zusammenlegung von Unternehmen finden Sie in KB 47626.
Ports	• UEM lokal: Überprüfen Sie, ob Port 1433 (TCP) und Port 1434 (UDP) auf Microsoft SQL Server freigegeben sind. • UEM Cloud: Port 8887 (TCP) muss zwischen dem lokalen UEM-Server und dem BlackBerry Connectivity Node geöffnet sein. Stellen Sie sicher, dass der vom Microsoft SQL Server verwendete Port, der die lokale UEM-Datenbank hostet, geöffnet und für den BlackBerry Connectivity Node zugänglich ist (z. B. Port 1433).

Bewährte Verfahren und Überlegungen zur Migration von UEM

Migration von IT-Richtlinien, Profilen und Gruppen

Objekt	Überlegungen und bewährte Verfahren
Von einem UEM-Quellserver kopierte Elemente	• Ausgewählte IT-Richtlinien • E-Mail-Profile • Wi-Fi-Profile • VPN-Profile • Proxy-Profile • BlackBerry Dynamics-Konnektivitätsprofile • BlackBerry Dynamics-Profile • Konfigurationseinstellungen für die App • Profile für Zertifizierungsstellenzertifikate • Profile für freigegebenes Zertifikat • Zertifikatsabruf • Profile für Benutzeranmelde-informationen • SCEP-Profile • CRL-Profile • OSCP-Profile • Zertifizierungsstelleneinstellungen (nur Entrust und PKI-Verbindung) • Clientzertifikate (App-Nutzung) • Alle Richtlinien und Profile, die mit den Richtlinien und Profilen verknüpft sind, die Sie auswählen
Elemente, die von einem Good Control-Quellserver nur zu UEM lokal kopiert wurden	• Richtliniensätze • Verbindungsprofile • App-Gruppen • App-Verwendung (für Zertifikate) • Zertifikate

Objekt	Überlegungen und bewährte Verfahren
Gruppenmigration	Benutzer, Rolle und Softwarekonfigurationszuordnungen werden nicht migriert. Sie müssen diese Zuweisungen manuell auf dem UEM-Zielserver neu erstellen.
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 UEM- oder -IT-Richtlinien oder -Profile migriert werden. Ändern Sie die IT-Quellrichtlinie entsprechend.
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.
BlackBerry Dynamics-Konnektivitätsprofile	Die Werte aus der Registerkarte „App-Server“ werden nicht migriert. Die Werte werden mit den Standardwerten des UEM-Zielservers aufgefüllt. Einige Werte aus der Registerkarte „Infrastruktur“ werden 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.
App-Gruppen (nur Good Control zu UEM lokal)	Die Gruppe „Jeder“ wird migriert, ihr sind aber keine Benutzer zugeordnet, und sie ist nicht mit der Gruppe „Alle Benutzer“ im UEM-Zielserver verknüpft.
Zertifikatsverwendung (UEM)	Zertifikatsverwendung wird migriert, ausgenommen: • Zertifikatsverwendungen, die bereits auf dem Zielserver vorhanden sind • Nicht-BlackBerry Dynamics-Apps • Benutzerdefinierte Apps von einer anderen Good Control-Organisation
Aufgaben nach der Migration für BlackBerry Dynamics-Benutzer	Führen Sie nach der Migration von Benutzern, Geräten, Gruppen und anderen Daten von Good Control zu lokalem UEM oder von einem lokalen UEM-Server zu UEM Cloud die folgenden Aufgaben aus: • Weisen Sie App-Konfigurationen BlackBerry Dynamics-Apps in Gruppen zu. • Weisen Sie Konnektivitätsprofile Gruppen zu. • Weisen Sie migrierte BlackBerry Dynamics-Richtlinien und Good Control-Konformitätsrichtlinien Benutzern zu. • Richten Sie Überschreibungsprofile ein (BlackBerry Dynamics-Profile und Konformitätsprofile). • Verschieben Sie JSON-Dateikonfigurationen von Good Control nach UEM. • Geben Sie in migrierten Verbindungsprofilen die Informationen für App-Server und BlackBerry Proxy-Cluster an.

Migrieren von Benutzern

Objekt	
Höchstanzahl von Benutzern	Sie können maximal 500 Benutzer gleichzeitig aus einem Quellserver migrieren. Wenn Sie mehr als die maximale Anzahl Benutzer für die Migration auswählen, wird nur die maximale Anzahl Benutzer migriert, und der Rest wird übersprungen. Sie können den Migrationsprozess nach Bedarf wiederholen, um alle Benutzer vom Quellserver zu migrieren.
E-Mail-Adresse	• Nur Benutzer mit einer verknüpften E-Mail-Adresse können migriert werden. • Benutzer, die eine im UEM-Zielserver bereits vorhandene E-Mail-Adresse verwenden, können nicht migriert werden. • Wenn zwei Benutzer in der Quelldatenbank die gleiche E-Mail-Adresse haben, wird nur ein Benutzer auf dem Bildschirm „Migrieren von Benutzern“ angezeigt.
Gruppen	• Sie können Benutzer ohne Gruppenzuordnung filtern, um diese Benutzergruppe bei einer Migration mit aufzunehmen. • Sie können keinen Benutzer migrieren, der Eigentümer einer freigegebenen Gerätegruppe ist. Dieser Benutzer erscheint nicht in der Liste der zu migrierenden Benutzer.
BlackBerry UEM Self-Service	• Nach der Migration muss der Benutzer die gleichen Anmeldedaten für BlackBerry UEM Self-Service verwenden, die er vor der Migration verwendet hat. • 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 BlackBerry UEM Self-Service hatten, erhalten nach der Migration nicht automatisch Berechtigung.

Migrieren von Geräten aus einem Quellserver

Objekt	Überlegungen und bewährte Verfahren
Konfiguration bestätigen	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.
Höchstanzahl von Geräten	Sie können maximal 2000 Geräte gleichzeitig aus einem Quellserver migrieren.
Benutzer	• Die Gerätebenutzer müssen in der UEM-Zieldomäne vorhanden sein. • Sie müssen alle Geräte eines Benutzers gleichzeitig migrieren.

Objekt	Überlegungen und bewährte Verfahren
Verwaltete iOS-Geräte aus einer UEM-Quelle	• Auf den Geräten muss die aktuelle Version von UEM Client installiert sein. • Geräte, denen ein App-Sperrprofil zugewiesen ist, können nicht migriert werden, weil UEM Client nicht für die Migration geöffnet werden kann. • Die Migration von Apple-DEP-Geräten wird nicht unterstützt. DEP-Geräte müssen auf die Werkseinstellungen zurückgesetzt und auf der neuen UEM-Instanz erneut aktiviert werden. Weitere Informationen finden Sie in KB 100525. • Geräte zur Benutzerregistrierung können nicht migriert werden. • Deaktivieren Sie in den App-Einstellungen für die entsprechenden Apps das Kontrollkästchen **Die App vom Gerät entfernen, wenn das Gerät von BlackBerry UEM entfernt wird**. Wenn Sie versuchen, ohne diesen Schritt zu migrieren, wird die App entfernt, und die Registrierung des Geräts in UEM wird möglicherweise aufgehoben.
Verwaltete Android-Geräte aus einer UEM-Quelle	• Auf den Android Enterprise-Geräten muss die aktuelle Version von UEM Client installiert sein. • Sie können Android-Geräte, die ein geschäftliches Profil haben, nicht über ein Google-Konto oder eine Google-Domäne migrieren.
Chrome OS-Geräte	Sie können Chrome OS-Geräte von einem UEM-Quellserver migrieren.
Geräte, die bei der Migration nicht unterstützt werden	• Windows • macOS
Freigegebene Ger\u00f4tegruppe	Ein Gerät, das zu einer freigegebenen Gerätegruppe gehört, kann nicht migriert werden. Diese Geräte werden nicht in der Migrationsliste angezeigt.

Objekt	Überlegungen und bewährte Verfahren
BlackBerry Dynamics-fähige Geräte	• 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. • BlackBerry Access for Windows, BlackBerry Access for macOS und BlackBerry BRIDGE werden bei der Migration nicht unterstützt. Nach Abschluss der Migration müssen Benutzer diese Apps erneut registrieren. • Der Migrationsprozess verfolgt oder garantiert nicht die Migration von UEM Client und Apps, die auf einem Gerät aktiviert werden, nachdem die Daten dieses Geräts zwischengespeichert wurden. Es wird empfohlen, den Benutzercache vor jeder Migration zu aktualisieren. • BlackBerry Dynamics-fähige Geräte werden immer auf dem Zielserver für BlackBerry Dynamics registriert. • Bei Migrationen von einer eigenständigen Good Control-Instanz werden Good Dynamics-MDM-Registrierungen nicht migriert. • Wenn ein Benutzer über mehrere Geräte mit BlackBerry Dynamics-Apps verfügt, werden alle Geräte automatisch für die Migration ausgewählt. • 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 vom UEM-Quellserver bezogen werden. Nachdem die Migration abgeschlossen wurde, muss der Schlüssel vom UEM-Zielserver abgerufen werden. • Um die Migration auf dem Gerät auszulösen, wird empfohlen, zuerst die App zu öffnen, die als Authentifikator auf dem Gerät konfiguriert ist.

Herstellen einer Verbindung zu einem Quellserver

Um Daten zu migrieren, müssen Sie BlackBerry UEM mit dem Quellserver verbinden. Sie können jeweils nur einen aktiven Quellserver haben.

Bevor Sie beginnen:

- Lesen Sie die Migrationsvoraussetzungen sowie Best Practices und Überlegungen.
- Stellen Sie in lokalen UEM-Umgebungen sicher, dass das mit Ihren Anmeldeinformationen verknüpfte Datenbankkonto über Schreibberechtigungen verfügt.
- Wenn in UEM Cloud-Umgebungen mehr als ein BlackBerry Connectivity Node aktiviert ist, konfigurieren Sie unbedingt alle BlackBerry Connectivity Node-Instanzen, sodass eine Verbindung zur gleichen Quelldatenbank hergestellt wird.

Befolgen Sie die Schritte für Ihre UEM-Umgebung:

Umgebung	Schritte
Lokales UEM	**a.** Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Migration > Konfiguration**. **b.** Klicken Sie auf +. **c.** Wählen Sie in der Dropdown-Liste **Quelltyp** den entsprechenden Typ des Quellservers aus. **d.** Geben Sie die Informationen für den Quellserver an. Wenn Sie Daten von einem Good Control-Quellserver migrieren, müssen Sie das Zertifikat nur exportieren und hochladen, wenn es nicht durch ein Drittanbieterzertifikat ersetzt wurde. UEM stuft Zertifikate von Drittanbietern prinzipiell als vertrauenswürdig ein. **e.** Klicken Sie auf **Verbindung testen**. **f.** Klicken Sie auf **Speichern**.
UEM Cloud	**a.** Klicken Sie in der Menüleiste der BlackBerry Connectivity Node-Verwaltungskonsole auf **Allgemeine Einstellungen > Migration**. **b.** Klicken Sie auf +. **c.** Geben Sie die Informationen für den Quellserver an. • Verwenden Sie für das Feld **Datenbankserver** das Format *<host>\<instance>* für einen dynamischen Port und *<host>:<port>* für einen statischen Port. • Wenn Sie Windows-NT-Authentifizierung auswählen, ändern Sie die Anmeldeeigenschaften des Diensts „BlackBerry UEM - BlackBerry Cloud Connector“, sodass sie auf dasselbe Konto verweisen, das auch zur Installation des Quellservers verwendet wurde. Ändern Sie nach Abschluss der Migration die Anmeldeeigenschaften wieder zu „Lokales Systemkonto verwenden“. **d.** Klicken Sie auf **Speichern**. **e.** Klicken Sie in der UEM-Verwaltungskonsole auf **Einstellungen > Migration > Konfiguration**. **f.** Klicken Sie auf +. **g.** Geben Sie einen Namen für die Quelldatenbank ein. **h.** Klicken Sie auf **Verbindung testen**. **i.** Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Führen Sie eine der folgenden Aktionen aus:

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

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

Bevor Sie beginnen: Herstellen einer Verbindung zu einem Quellserver.

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

Wenn Sie mehr als einen Quellserver in einer lokalen UEM-Umgebung konfiguriert haben, wählen Sie den Quellserver aus, von dem Sie Daten migrieren möchten.

2. Klicken Sie auf **IT-Richtlinien, Profile, Gruppen**.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie die Elemente aus, die Sie migrieren möchten.

   Der Name des Quellservers wird an den Namen jeder Richtlinie und jedes Profils angehängt, wenn diese zum Zielserver migriert wurden.
5. Klicken Sie auf **Vorschau**.
6. Klicken Sie auf **Migrieren**.

Wenn Sie fertig sind:

- Um die IT-Richtlinien, Profile und Gruppen zu konfigurieren, klicken Sie auf **IT-Richtlinien und -Profile konfigurieren**. Der Bildschirm **Richtlinien und Profile** wird geöffnet.
- 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.
- Migrieren von Benutzern aus einem Quellserver.

Migrieren von Benutzern aus einem Quellserver

Bevor Sie beginnen:

- Herstellen einer Verbindung zu einem Quellserver.
- Migrieren von IT-Richtlinien, Profilen und Gruppen aus einem Quellserver.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Migration > Benutzer**.
2. Klicken Sie auf **Cache aktualisieren**.

   Die Aktualisierung dauert für 1000 Benutzer etwa zehn Minuten. Das Aktualisieren des Caches ist nur für den ersten Satz Benutzer erforderlich, die Sie migrieren wollen. Wenn Sie während einer Migration Änderungen am Quellserver vornehmen, sollten Sie den Cache erneut aktualisieren.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie die Benutzer aus, die Sie migrieren möchten.

   Standardmäßig werden nur die ersten 20.000 Benutzer angezeigt. Sie können nach Bedarf nach bestimmten Benutzern suchen. Beachten Sie, dass bei Auswahl aller Benutzer nur die Benutzer ausgewählt werden, die auf der ersten Seite angezeigt werden.
5. Klicken Sie auf **Weiter**.
6. Weisen Sie den ausgewählten Benutzern eine IT-Richtlinie, Gruppen und Profile zu.
7. Klicken Sie auf **Vorschau**.
8. Klicken Sie auf **Migrieren**.

Beachten Sie, dass migrierte Benutzerkonten nicht vom Quellserver entfernt werden.

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

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:

- Herstellen einer Verbindung zu einem Quellserver.
- Migrieren von IT-Richtlinien, Profilen und Gruppen aus einem Quellserver.
- Migrieren von Benutzern aus einem Quellserver.
- Benachrichtigen Sie Benutzer von iOS-Geräten darüber, dass der BlackBerry UEM Client geöffnet werden und bis zum Abschluss der Migration geöffnet bleiben muss.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Migration > Geräte**.
2. Klicken Sie auf **Cache aktualisieren**.

   Die Aktualisierung dauert für 1000 Geräte etwa zehn Minuten. Das Aktualisieren des Caches ist nur für den ersten Satz der Geräte erforderlich, die Sie migrieren wollen. Wenn Sie während einer Migration Änderungen am Quellserver vornehmen, sollten Sie den Cache erneut aktualisieren.
3. Klicken Sie auf **Weiter**.
4. Auswahl der Geräte, die Sie migrieren möchten.

   Standardmäßig werden nur die ersten 20.000 Geräte angezeigt. Sie können nach Bedarf nach bestimmten Geräten suchen. Beachten Sie, dass bei Auswahl aller Geräte nur die Geräte ausgewählt werden, die auf der ersten Seite angezeigt werden.
5. Klicken Sie auf **Vorschau**.
6. Klicken Sie auf **Migrieren**.
7. Klicken Sie auf **Migration** > **Status**.

Wenn Sie fertig sind: Um den Status der zu migrierenden Geräte anzuzeigen, klicken Sie auf **Migration > Status**.

Konfigurieren der Netzwerkkommunikation und Eigenschaften für BlackBerry Dynamics-Apps

Befolgen Sie die Anweisungen in diesem Abschnitt, um die Netzwerkkommunikation und andere Eigenschaften für BlackBerry Dynamics-Apps zu konfigurieren.

Aufgabe	Beschreibung
Verwalten von BlackBerry Proxy-Clustern.	Erstellen und Verwalten von BlackBerry Proxy-Clustern, die Daten für BlackBerry Dynamics-Apps weiterleiten.
Konfigurieren von Direct Connect über Portweiterleitung.	Konfigurieren von Direct Connect für BlackBerry Proxy-Instanzen.
Konfigurieren von BlackBerry Dynamics-Eigenschaften (nur lokal).	Konfigurieren Sie Eigenschaften für die BlackBerry Dynamics-Apps, die Sie in der Unternehmensumgebung bereitstellen möchten.
Konfigurieren Sie die Kommunikationseinstellungen für BlackBerry Dynamics-Apps (nur lokal).	Konfigurieren Sie die Kommunikationseinstellungen für die BlackBerry Dynamics-Apps, die Sie in der Unternehmensumgebung bereitstellen möchten, einschließlich des Kommunikationsprotokolls, das von den Apps verwendet wird.
Senden von BlackBerry Dynamics-App-Daten über einen HTTP-Proxy.	Konfigurieren Sie UEM so, dass BlackBerry Dynamics-App-Daten zwischen BlackBerry Proxy und einem Anwendungsserver über einen HTTP-Proxy gesendet werden.
Methoden zur Weiterleitung des Datenverkehrs für BlackBerry Dynamics-Apps.	Details zu den verschiedenen Methoden, mit denen Sie Datenverkehr für BlackBerry Dynamics-Apps weiterleiten können.
Konfigurieren der Kerberos-Authentifizierung für BlackBerry Dynamics-Apps (nur lokal).	Konfigurieren Sie die eingeschränkte Kerberos-Delegierung oder Kerberos PKINIT, um die Authentifizierung für Benutzer zu vereinfachen.

Weitere Informationen zum Bereitstellen und Verwalten von BlackBerry Dynamics-Apps finden Sie unter Verwalten von BlackBerry Dynamics-Apps in der Dokumentation für Administratoren.

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. Sie 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 > Cluster**.
2. 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 **OK**.
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 das Cluster. **b.** Klicken Sie auf **Entfernen**.
Legen Sie App-Proxyeinstellungen für ein Cluster fest.	**a.** Klicken Sie auf den Clusternamen. **b.** Klicken Sie auf **Globale Einstellungen überschreiben**. **c.** Siehe Konfigurieren der Proxyeinstellungen der BlackBerry Dynamics-App.
Laden Sie PAC-Dateiaktualisierungen für alle Cluster herunter.	Klicken Sie auf **PAC-Cache aktualisieren**.
Geben Sie ein vertrauenswürdiges Stammzertifikat an, um PAC-Dateien vom Server herunterzuladen.	**a.** Vergewissern Sie sich, dass das Zertifikat im X.509-Format (*.cer, *.der) in einem Netzwerkpfad gespeichert ist, auf den Sie über die Verwaltungskonsole zugreifen können. **b.** Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Vertrauenswürdige Zertifikate**. **c.** Klicken Sie auf + neben **PAC-Server-Vertrauensstellungen**. **d.** Klicken Sie auf **Durchsuchen**. **e.** Navigieren Sie zum zu analysierenden Zertifikat, und wählen Sie es aus. **f.** Klicken Sie auf **Öffnen**. **g.** Geben Sie eine Beschreibung für das Zertifikat ein. **h.** Klicken Sie auf **Hinzufügen**.
Aktivieren Sie einen BlackBerry Proxy, der für die Aktivierung verwendet werden soll (nur lokale UEM).	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 über Portweiterleitung

Bevor Sie beginnen:

- Konfigurieren Sie einen öffentlichen DNS-Eintrag für jeden BlackBerry Connectivity Node-Server (z. B. bp01.mydomain.com, bp02.mydomain.com usw.).
- Konfigurieren Sie die externe Firewall so, dass eingehende Verbindungen auf Port 17533 zulässig sind, und verwenden Sie diesen Port für die Weiterleitung an den jeweiligen BlackBerry Connectivity Node-Server.
- Wenn die BlackBerry Connectivity Node-Instanzen in einer DMZ installiert sind, stellen Sie sicher, dass die entsprechenden Ports zwischen jedem BlackBerry Connectivity Node und allen Anwendungsservern geöffnet sind, auf die die BlackBerry Dynamics-Apps zugreifen müssen (z. B. Microsoft Exchange, interne Webserver und BlackBerry UEM Core).

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Direct Connect**.
2. Klicken Sie auf eine BlackBerry Proxy-Instanz.
3. Um Direct Connect zu aktivieren, markieren Sie das Kontrollkästchen **Direct Connect aktivieren**. Überprüfen Sie im Feld **BlackBerry Proxy-Hostname** den Hostnamen auf Richtigkeit. Wenn der von Ihnen erstellte öffentliche DNS-Eintrag vom FQDN des Servers abweicht, geben Sie stattdessen den externen FQDN an.
4. Wiederholen Sie die Schritte für alle BlackBerry Proxy-Instanzen im Cluster.

   Um nur einige BlackBerry Proxy-Instanzen für Direct Connect zu aktivieren, erstellen Sie ein neues BlackBerry Proxy-Cluster. Alle Server in einem Cluster müssen dieselbe Konfiguration aufweisen. Weitere Informationen finden Sie unter Verwalten von BlackBerry Proxy-Clustern.
5. Klicken Sie auf **Speichern**.

Konfigurieren von BlackBerry Dynamics-Eigenschaften

Bei einer lokalen UEM-Umgebung können Sie verschiedene Eigenschaften konfigurieren, die sich auf die Sicherheit, das Verhalten und die Kommunikation von BlackBerry Dynamics-Apps beziehen.

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

Aufgabe	Schritte
Ändern Sie globale Eigenschaften für BlackBerry Dynamics-Apps.	• Klicken Sie auf **Globale Eigenschaften**. • Konfigurieren Sie die Eigenschaften nach Bedarf. Siehe Globale Eigenschaften von BlackBerry Dynamics. • Klicken Sie auf **Speichern**.
Ändern Sie die BlackBerry Dynamics-Eigenschaften für einen bestimmten UEM-Server.	• Klicken Sie auf **Eigenschaften**. • Klicken Sie in der Dropdown-Liste **Servertyp** auf **BlackBerry Control-Server** und wählen den UEM-Server, den Sie konfigurieren möchten. • Konfigurieren Sie die Eigenschaften nach Bedarf. Siehe BlackBerry Dynamics-Eigenschaften. • Klicken Sie auf **Speichern**.

Aufgabe	Schritte
Ändern Sie die Eigenschaften für eine BlackBerry Proxy-Instanz.	• Klicken Sie auf **Eigenschaften**. • Klicken Sie in der Dropdown-Liste **Servertyp** auf **BlackBerry Proxy-Server** und wählen den BlackBerry Proxy-Server, den Sie konfigurieren möchten. • Konfigurieren Sie die Eigenschaften nach Bedarf. Siehe BlackBerry Proxy-Eigenschaften. • 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.

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 des Schlüsselspeichers der PKCS 12-Zertifikate, die Gerätebenutzer zum Signieren von E-Mail-Nachrichten und für die Client-Authentifizierung hochladen können, in Sekunden. Diese Eigenschaft ist schreibgeschützt und kann nicht geändert werden.	86400	—

Kommunikation

Eigenschaft	Beschreibung	Standard	Neu starten
cntmgmt.internal.port	Der interne Port für den Containerverwaltungsdienst.	17317	Ja
cntmgmt.max.conns.above.limit	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 BlackBerry Technical Support.	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 BlackBerry Technical Support.	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 BlackBerry Technical Support.	0	Ja
cntmgmt.max.read.throughput	Die maximale Anzahl gleichzeitiger Lesevorgänge für die Containerverwaltung. **Hinweis:** Ändern Sie diese Einstellung nicht ohne Rücksprache mit dem BlackBerry Technical Support.	500	Ja
cntmgmt.max.write.throughput	Die maximale Anzahl gleichzeitiger Schreibvorgänge für die Containerverwaltung. **Hinweis:** Ändern Sie diese Einstellung nicht ohne Rücksprache mit dem BlackBerry Technical Support.	500	Ja
cntmgmt.ssl.external.enable	Steuert die SSL-Aktivierung für die externe Containerverwaltung. Diese Eigenschaft ist schreibgeschützt und kann nicht geändert werden.	Aktiviert	—
cntmgmt.ssl.internal.enable	Steuert die SSL-Aktivierung für die interne Containerverwaltung. Diese Eigenschaft ist schreibgeschützt und kann nicht geändert werden.	Aktiviert	—

Doppelte Container

Wenn 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 UEM-Protokolldatei erfasst.

Eigenschaft	Beschreibung	Standard	Neu starten
Automatisches Entfernen älterer, doppelter Container auf demselben Gerät für den Benutzer nach der Bereitstellung	Legen Sie fest, ob 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 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 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) 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 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 UEM bis zum erneuten Senden einer nicht bestätigen Nachricht in Sekunden an.	60	Ja
config.command.retry	Gibt an, wie häufig (in Sekunden) UEM den Vorgang zum Erkennen und erneuten Senden nicht bestätigter Nachrichten ausführt. Wenn diese Eigenschaft auf 0 gesetzt wird, führt 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) UEM Konformitätsrichtlinien für alle Richtliniendatensätze abruft.	1440	Ja

Inaktive Container löschen

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

Container, für die ein Authentifikator konfiguriert ist, werden bei diesem Prozess nicht gelöscht.

Eigenschaft	Beschreibung	Standard	Neu starten
Auftrag für automatisches Entfernen von inaktiven Containern aktivieren (ein/aus)	Legen Sie fest, ob 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 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) 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
gc.purge.dbJobs Serveraufträge löschen	Legen Sie fest, ob Serveraufträge von UEM in regelmäßigen Abständen automatisch gelöscht werden.	Aktiviert	Ja
gc.purge.dbJobs.interval Serverjobintervall löschen	Wenn „Serveraufträge löschen“ aktiviert ist, legen Sie fest, wie häufig (in Tagen) Serveraufträge von UEM gelöscht werden.	30	Ja

BlackBerry Dynamics-Eigenschaften

Eingeschränkte Kerberos-Delegierung

Eigenschaft	Beschreibung	Standard	Neu starten
Speicherort der Datei „krb5.conf“ auf dem GC-Server (gc.krb5.config.file)	Der Speicherort der Datei krb5.conf, die benötigt wird, um KCD zu konfigurieren und die bereichsübergreifende Authentifizierung zu aktivieren, wenn eine CAPATH-Vertrauensbeziehung mit mehreren Kerberos-Domains besteht.	Nicht festgelegt	Ja
KCD-Debugging-Modus aktivieren (gc.krb5.debug)	Gibt an, ob 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
Speicherort der Schlüsseltabellendatei (gc.krb5.keytab.file)	Der Speicherort der Kerberos-Schlüsseltabellendatei auf dem Computer, der BlackBerry UEM hostet.	Nicht festgelegt	Ja

Eigenschaft	Beschreibung	Standard	Neu starten
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 folgende Tabelle beschreibt 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.	15000	—
gp.gps.dns.server.ttl.ms	Zeit, die auf Antwort des DNS-Servers gewartet wird, in Millisekunden.	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	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
gps.directconnect.supported.ciphers	Hiermit lassen sich Verschlüsselungssammlungen zur Verschlüsselung von Bridging und Kommunikation über BlackBerryDirect Connect hinzufügen oder ändern. Sie können festlegen, dass Ihr eigener Proxyserver für Direct Connect konfiguriert und zwischen Client-Geräten und dem BlackBerry Proxy-Server platziert werden soll. Wenn Sie einen eigenen Proxyserver hinzugefügt haben, stellen Sie sicher, dass die BlackBerry Proxy Server-Verschlüsselungen denen entsprechen, die von Ihrem eigenen Proxyserver benötigt werden. Alle Verschlüsselungen müssen von Java unterstützt werden.	In der Benutzerob aufgeführt	Ja
gp.directconnect. supported.protocols	Hiermit lassen sich die kryptografischen Protokolle, die von der Direct-Connect-Bridge des Systems unterstützt werden sollen, hinzufügen oder ändern.	TLSv1, TLSv1.1, TLSv1.2	Ja
gp.eacp.command.service.nslookup. srv.ldap	Ermöglicht LDAP über TCP für Active Directory-Server. Active Directory-Server bieten den LDAP-Dienst über das TCP-Protokoll an. Clients suchen einen LDAP-Server, indem sie DNS nach einem Datensatz in der Form _ldap._tcp.DnsDomainName abfragen. 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.server.secure.ciphers	Hiermit lassen sich Verschlüsselungssammlungen, die die Kommunikation über einen BlackBerry Proxy-Server verschlüsseln, hinzufügen oder ändern. Alle Verschlüsselungen müssen von Java unterstützt werden.	In der Benutzerob aufgeführt	—

Eigenschaft	Beschreibung	Standard	Neu starten
gp.server.secure.protocols	Hiermit lassen sich die kryptografischen Protokolle, die von Ihrem BlackBerry Proxy-Server unterstützt werden sollen, hinzufügen oder ändern.	TLSv1.2	—

Konfigurieren Sie die Kommunikationseinstellungen für BlackBerry Dynamics-Apps

Bei lokalen UEM-Umgebungen können Sie 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 ist nur TLS v1.2 zulässig. Sie können auch TLSv1 und v1.1 zulassen. Sie müssen mindestens ein Protokoll auswählen.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Kommunikationseinstellungen**.
2. Konfigurieren Sie die Einstellungen nach Bedarf.
3. Klicken Sie auf **Speichern**.

Senden von BlackBerry Dynamics-App-Daten über einen HTTP-Proxy

Sie können BlackBerry UEM so konfigurieren, dass BlackBerry Dynamics-App-Daten zwischen BlackBerry Proxy und einem Anwendungsserver über einen HTTP-Proxy gesendet werden. BlackBerry Dynamics-Apps unterstützen sowohl manuelle Proxyeinstellungen als auch PAC-Dateien für Verbindungen zu Anwendungsservern. Für die Verwendung einer PAC-Datei müssen Apps mit BlackBerry Dynamics SDK 7.0 oder höher entwickelt werden. Wenn Sie sowohl manuelle als auch PAC-Dateieinstellungen konfigurieren, hat die PAC-Datei bei Apps, die sie unterstützen, Vorrang. Apps, die mit einer älteren BlackBerry Dynamics SDK-Version entwickelt wurden, verwenden die manuellen Einstellungen.

BlackBerry Access unterstützt zudem manuelle Proxy- und App-Konfigurationseinstellungen der PAC-Datei, die nur für Suchfunktionen mit BlackBerry Access gelten. Proxy-Konfigurationseinstellungen für BlackBerry Access oder andere Apps mit separaten Proxyeinstellungen überschreiben die UEM-Proxyeinstellungen. Weitere Informationen finden Sie im Administrationshandbuch für BlackBerry Access.

Überlegungen zur Verwendung einer PAC-Datei mit BlackBerry Proxy

Überlegungen	Details
Unterstützte PAC-Dateianweisungen	• DIRECT • PROXY (als HTTPS-Proxy behandelt; Verbindung wird über HTTP CONNECT hergestellt) • HTTPS (Verbindung wird über HTTP CONNECT hergestellt)

Überlegungen	Details
Nicht unterstützte PAC-Dateianweisungen	Ein Verbindungsfehler tritt bei folgenden Elementen auf: • SOCKS • SOCKS4 • SOCKS5 • HTTP • Benutzerdefiniertes „NATIVE“-Verzeichnis definiert von BlackBerry Access BLOCK-Dateianweisungen werden als DIREKT behandelt.
Einschränkungen	• Die dnsDomainIs-Funktion darf nicht die Zeichen „_“ und „*“ enthalten. • Die shExpMatch-Funktion darf nicht die Ausdrücke „[0-9]“, „?“, „/^d“ oder „d +“ enthalten. • Die Option zum Entfernen des Pfads und der Abfrage aus dem URI wird nicht unterstützt.
PAC-Cache	BlackBerry Proxy lädt die PAC-Datei herunter und speichert sie im Cache, um die Leistung zu verbessern. Der PAC-Cache wird alle 24 Stunden aktualisiert. Wenn Sie den Cache manuell aktualisieren möchten, gehen Sie in der Verwaltungskonsole zu Einstellungen > Infrastruktur > BlackBerry Router und Proxy > Globale Einstellungen, und klicken Sie auf PAC-Cache aktualisieren.

Konfigurieren der Proxyeinstellungen der BlackBerry Dynamics-App

1. Führen Sie die entsprechenden Schritte für Ihre UEM-Umgebung aus:

Umgebung	Aufgabe
Lokales UEM	Führen Sie folgende Aktionen in der UEM-Verwaltungskonsole aus: • Wenn Sie globale App-Proxyeinstellungen festlegen möchten, klicken Sie auf **Einstellungen > Infrastruktur > BlackBerry Router und Proxy**, und erweitern Sie **Globale Einstellungen**. • Wenn Sie App-Proxyeinstellungen für einen Cluster festlegen möchten, klicken Sie auf **Einstellungen > BlackBerry Dynamics > Cluster**. Klicken Sie auf den Namen eines Clusters, und aktivieren Sie das Kontrollkästchen **Globale Einstellungen überschreiben**. • Wenn Sie manuelle App-Proxyeinstellungen für einen Server festlegen möchten, klicken Sie auf **Einstellungen > Infrastruktur > BlackBerry Router und Proxy**. Erweitern Sie einen Server, und aktivieren Sie das Kontrollkästchen **Globale Einstellungen überschreiben**. Beachten Sie, dass PAC-Dateien nicht unterstützt werden, wenn globale Proxyeinstellungen für einen Server überschrieben werden.
UEM Cloud	Klicken Sie in der BlackBerry Connectivity Node-Verwaltungskonsole auf **Allgemeine Einstellungen > BlackBerry Router und Proxy > Globale Einstellungen**.

2. Wählen Sie die entsprechende Option aus, und führen Sie die erforderlichen Schritte aus:

Option	Schritte
HTTP-Proxy manuell aktivieren	**a.** Wählen Sie die entsprechende Proxykonfiguration. Wenn Sie einen Proxy verwenden möchten, um eine Verbindung mit den angegebenen Servern herzustellen, klicken Sie auf +, um Server hinzuzufügen. **b.** Geben Sie die Adresse des Proxyservers und die Portnummer an, die vom Proxyserver überwacht wird. **c.** Wenn für den Proxyserver eine Authentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Authentifizierung verwenden**, und geben Sie die Zugangsdaten für die Authentifizierung an.
PAC aktivieren	Geben Sie im Feld **PAC-URL** die URL für die PAC-Datei ein. Wenn die in der PAC-Datei angegebenen Proxys eine Authentifizierung erfordern, aktivieren Sie das Kontrollkästchen **Proxy-Authentifizierung unterstützen**, und geben Sie die Zugangsdaten für die Authentifizierung an. Zugangsdaten für die Endbenutzerauthentifizierung werden für die Proxyauthentifizierung nicht unterstützt.

3. Klicken Sie auf **Speichern**.

Methoden zur Weiterleitung des Datenverkehrs für BlackBerry Dynamics-Apps

BlackBerry UEM verfügt über mehrere Optionen, mit denen Sie steuern können, wie BlackBerry Dynamics-Datenverkehr weitergeleitet wird. Standardmäßig wird der gesamte BlackBerry Dynamics-App-Datenverkehr ohne Web-Proxyserver-Konfigurationen direkt zum Internet geleitet. In diesem Abschnitt werden nur Konfigurationen behandelt, die sich auf die allgemeine Weiterleitung auswirken.

Die Weiterleitung für BlackBerry Dynamics-Apps kann durch die folgenden Konfigurationen geändert werden:

Konfiguration	Details
Zugewiesenes BlackBerry Dynamics-Konnektivitätsprofil	• Im standardmäßigen BlackBerry Dynamics-Konnektivitätsprofil ist nur das Element „Standardmäßig zulässiger Domänen-Routingtyp“ konfiguriert, das auf „Direkt“ festgelegt ist. • Bei Verwendung des standardmäßigen BlackBerry Dynamics-Konnektivitätsprofils sind keine internen Server oder Domänen für BlackBerry Dynamics-Apps zugänglich. Sie können das Standard-Konnektivitätsprofil ändern oder ein neues Profil erstellen, um Verbindungen zu internen Servern zu ermöglichen. • Weitere Informationen finden Sie unter Erstellen eines BlackBerry Dynamics-Konnektivitätsprofils in der Dokumentation für Administratoren.

Konfiguration	Details

Web-Proxyserver-Konfiguration für BlackBerry Proxy	• Standardmäßig ist BlackBerry Proxy nicht für den Einsatz eines Web-Proxyservers konfiguriert. Jeder BlackBerry Proxy-Server versucht, eine direkte Verbindung zum Internet herzustellen. Dies gilt sowohl für den Datenverkehr des App-Servers als auch für BlackBerry Dynamics NOC-Verbindungen.
	• Informationen zum Konfigurieren von BlackBerry Proxy finden Sie unter Senden von BlackBerry Dynamics-App-Daten über einen HTTP-Proxy.
	• Im BlackBerry Dynamics-Konnektivitätsprofil können Sie die Server angeben, auf die die BlackBerry Dynamics-Apps über die Firewall mit BlackBerry Proxy zugreifen können. Weitere Informationen finden Sie unter Erstellen eines BlackBerry Dynamics-Konnektivitätsprofils in der Dokumentation für Administratoren.
	• Durch das Weiterleiten des Datenverkehrs über BlackBerry Proxy können Webbrowser und BlackBerry Dynamics-Apps auf Geräten eine Verbindung zu jedem Server hinter der Firewall herstellen, der von BlackBerry Proxy erreichbar ist, und Sie können den Datenverkehr zwischen BlackBerry Dynamics-Apps und den Ressourcen Ihres Unternehmens einfach überwachen.
	• Beachten Sie Folgendes, wenn Sie sich für die Weiterleitung von Daten über einen BlackBerry Proxy-Server entscheiden:
	  • Das Herstellen von Verbindungen zu Servern im Internet kann länger dauern.
	  • Wenn Sie einen Web-Proxy für den Zugriff auf externe Sites nutzen und Ihren Proxy so konfiguriert haben, dass bestimmte Websites eingeschränkt werden, müssen Sie auch die Proxy-Eigenschaften in BlackBerry Proxy einstellen, wenn sie die Option „Gesamten Datenverkehr weiterleiten“ auswählen. Ansonsten können die Apps nicht auf externe Websites zugreifen.
	  • BlackBerry Access kann mit einer PAC-Datei konfiguriert werden, die die zulässigen Websites bestimmt. In diesem Fall bestimmt die PAC-Datei die Proxy-Einstellungen. Weitere Informationen finden Sie im Administrationshandbuch für BlackBerry Access.

App-spezifische Einstellungen	• Eine App-spezifische Konfiguration kann erforderlich sein, damit Apps eine Verbindung zu bestimmten Servern herstellen können (z. B. für BlackBerry Work konfiguriert mit der URL von Microsoft Exchange Server). Lesen Sie die Dokumentation zu BlackBerry Dynamics-Apps, um zu erfahren, welche App-Konfigurationen angewendet werden müssen. • BlackBerry Access und einige Drittanbieter-Apps erlauben die Konfiguration des Web-Proxyservers auf Anwendungsebene. Bei der Standardkonfiguration für BlackBerry Access wurde kein Web-Proxyserver konfiguriert. • Ein App-Server ist ein Server, mit dem sich eine BlackBerry Dynamics-App verbindet, z. B. der URL eines Microsoft Exchange Server, die URL für BEMS, die URL für Skype for Business oder eine beliebige URL, die BlackBerry Access durchsucht. Der BlackBerry Dynamics NOC und der BlackBerry UEM Core-Server sind keine App-Server.

Wenn Sie ein BlackBerry Dynamics-Konnektivitätsprofil und eine Web-Proxykonfiguration für BlackBerry Proxy-Server konfigurieren und zuweisen, wird das BlackBerry Dynamics-Konnektivitätsprofil immer zuerst geprüft. Wenn der Datenverkehr am BlackBerry Proxy-Server eingeht, wird die auf dem BlackBerry Proxy-Server festgelegte PAC- oder Web-Proxyserver-Konfiguration auf Konnektivität überprüft. Mit der Konfiguration eines Web-Proxys auf dem BlackBerry Proxy-Server wird gesteuert, wie der BlackBerry Proxy Datenverkehr an das Internet sendet. Dies hat keinen Einfluss darauf, wie die BlackBerry Dynamics-App auf dem Gerät Verbindungen bewertet.

Beispiel für Weiterleitungsszenarien für BlackBerry Dynamics-Datenverkehr

Die folgenden Szenarien sind Beispiele für gängige Konfigurationen:

Szenario	BlackBerry Dynamics-Konnektivitätsprofil	Web-Proxy-Konfiguration für BlackBerry Proxy	App-spezifische Einstellungen
Weiterleiten des Datenverkehrs an bestimmte Server oder Domänen über BlackBerry Proxy. Geeignet für Szenarien, in denen einige interne App-Server für BlackBerry Dynamics-Apps zugänglich sein müssen, der allgemeine Datenverkehr zu öffentlichen Servern jedoch direkt bleiben kann.	• Standardmäßig zulässiger Domänen-Routingtyp: Direkt • Zulässige Domänen: Fügen Sie die internen Domänen hinzu, die Sie über BlackBerry Proxy weiterleiten möchten, und wählen Sie ein Cluster aus. • Zusätzliche Server: Fügen Sie bei Bedarf bestimmte Servernamen hinzu, und wählen Sie ein Cluster aus.	Keine Konfiguration erforderlich.	Keine Konfiguration erforderlich.
Weiterleiten des gesamten Datenverkehrs über BlackBerry Proxy und dann über einen Web-Proxyserver. Geeignet für Unternehmen, die den gesamten Datenverkehr von geschäftlichen Apps intern weiterleiten müssen.	Standardmäßig zulässiger Domänen-Routingtyp: BlackBerry Proxy-Cluster	Verwenden Sie eine manuelle Web-Proxyserver-Konfiguration oder eine PAC-Datei.	Keine Konfiguration erforderlich.

Szenario	BlackBerry Dynamics-Konnektivitätsprofil	Web-Proxy-Konfiguration für BlackBerry Proxy	App-spezifische Einstellungen
Einen Teil des Datenverkehrs für die meisten Apps intern weiterleiten, speziell für das Surfen im Internet mit BlackBerry Access aber einen Proxyserver konfigurieren. Geeignet für Unternehmen, die den Datenverkehr für Apps intern, aber Browser-Datenverkehr über einen Web-Proxy-Server weiterleiten müssen.	• Standardmäßig zulässiger Domänen-Routingtyp: Direkt • Zulässige Domänen: Fügen Sie die internen Domänen hinzu, die Sie über BlackBerry Proxy weiterleiten möchten, und wählen Sie ein Cluster aus. • Zusätzliche Server: Fügen Sie bei Bedarf bestimmte Servernamen hinzu, und wählen Sie ein Cluster aus.	Wenn BlackBerry Proxy-Server keinen direkten Zugriff auf das Internet haben oder wenn ein Proxy für BlackBerry Dynamics NOC-Verbindungen erforderlich ist, konfigurieren Sie nach Bedarf einen Web-Proxy-Server.	Wählen Sie in der App-Konfiguration für BlackBerry Access die Option „Web-Proxy aktivieren“ und „Automatische Proxy-Konfiguration verwenden“ aus.

Konfigurieren der Kerberos-Authentifizierung für BlackBerry Dynamics-Apps

In einer lokalen BlackBerry UEM-Umgebung unterstützen BlackBerry Dynamics-Apps die eingeschränkte Kerberos-Delegierung (KCD) und Kerberos PKINIT. Sie können KCD oder Kerberos PKINIT für BlackBerry Dynamics-Apps unterstützen, jedoch nicht beide.

Kerberos-Authentifizierung	Beschreibung
KCD	KCD ermöglicht Benutzern den Zugriff auf Unternehmensressourcen ohne Eingabe Ihrer Netzwerkanmeldedaten. KCD verwendet Service-Tickets, die durch Schlüssel verschlüsselt und entschlüsselt werden, in denen die Anmeldedaten des Benutzers nicht enthalten sind. Wenn Sie KCD konfigurieren, delegiert die BlackBerry Dynamics-App die Authentifizierung an UEM, um Zugriff auf eine geschäftliche Ressource zu erhalten. Sie können die Netzwerkressourcen einschränken, auf die Benutzer zugreifen können, indem Sie das Konto, das UEM verwendet, so konfigurieren, dass es nur für bestimmte Dienste vertrauenswürdig ist. Wenn beispielsweise KCD nicht konfiguriert ist und eine App eine Ressource wie mypage.mydomain.com anfordert, fordert die App den Benutzer zur Eingabe von Anmeldeinformationen auf. Wenn KCD konfiguriert ist, verarbeitet die BlackBerry Dynamics-Infrastruktur die Authentifizierung, und der Benutzer wird nicht zur Eingabe von Anmeldeinformationen aufgefordert. Siehe Voraussetzungen für die Konfiguration von KCD für BlackBerry Dynamics-Apps und Konfigurieren von KCD für BlackBerry Dynamics-Apps.
Kerberos PKINIT	Kerberos PKINIT-Authentifizierung etabliert die vertrauenswürdige Verbindung zwischen der BlackBerry Dynamics-App und der Windows-KDC. Die Benutzerauthentifizierung basiert auf Zertifikaten, die von Microsoft Active Directory-Zertifikatdiensten ausgegeben werden. Siehe Anforderungen zur Unterstützung von Kerberos PKINIT für BlackBerry Dynamics-Apps.

Voraussetzungen für die Konfiguration von KCD für BlackBerry Dynamics-Apps

Objekt	Beschreibung
Active Directory-Port	Port 88 auf dem Active Directory-Dienst muss für alle UEM-Server zugänglich sein.
Kerberos -Umgebung	Die Kerberos-Umgebung muss die folgenden Komponenten enthalten: • Microsoft Active Directory-Server: Der Verzeichnisdienst, der alle Benutzer und Computer authentifiziert und autorisiert, die mit dem Windows-Netzwerk verbunden sind. • Kerberos Key Distribution Center (KDC): Der Authentifizierungsdienst auf dem Active Directory-Server, der Sitzungstickets und -schlüssel für Benutzer und Computer in der Active Directory-Domäne bereitstellt. • Um KCD mit Microsoft 365-Ressourcen zu verwenden, muss die lokale Active Directory-Domain mit Entra integriert sein. Weitere Informationen finden Sie im Microsoft-Artikel „Integrieren von lokalem AD mit Entra“.

Objekt	Beschreibung

krb5.conf-Datei	Ihre UEM-Umgebung erfordert eine krb5.conf-Datei mit spezifischen Werten für Ihr KDC. Sie muss folgende Mindesteinstellungen enthalten:
	
	RC4-Verschlüsselung:
	
	`[libdefaults]`
	`allow_weak_crypto = true`
	`forwardable = true`
	
	AES-Schlüsseltabellendatei:
	
	`[libdefaults]`
	`forwardable = true`
	
	Wenn Sie eine AES-Schlüsseltabellendatei verwenden, müssen Sie die Datei mit dem AES-Flag `/crypto AES256-SHA1` erstellen:
	
	`ktpass /out outfilename.keytab /mapuser kerberos_account@REALM_IN_ALL_CAPS /princ kerberos_account@REALM_IN_ALL_CAPS /pass kerberos_account_password /ptype KRB5_NT_PRINCIPAL / crypto AES256-SHA1`
	
	Sie müssen den Speicherort der krb5.conf-Datei unter Einstellungen > BlackBerry Dynamics > Eigenschaften (siehe Konfigurieren von KCD für BlackBerry Dynamics-Apps) angeben. Weitere Informationen zum Erstellen einer krb5.conf-Datei finden Sie in der Dokumentation zu MIT Kerberos.

Dienstprinzipalnamen (Service Principal Name, SPN)	Erstellen Sie SPNs für alle HTTP-Dienste, einschließlich BlackBerry Enterprise Mobility Server. Sie müssen für jede Zielressource, auf die Geräte zugreifen sollen, einen SPN festlegen. Weitere Informationen zum Erstellen und Ändern von SPNs finden Sie unter Einen Service Principal Name für Kerberos-Verbindungen registrieren.

Objekt	Beschreibung
Kerberos-Umgebungen mit mehreren Bereichen	• Mindestens ein UEM Core muss in jedem Kerberos-Bereich installiert sein. UEM muss sich in demselben Kerberos-Bereich wie die Ressource befinden, weil eine bereichsübergreifende Ressourcendelegierung nicht unterstützt wird. • Stellen Sie sicher, dass KCD mit einem einzelnen Bereich funktioniert, bevor Sie KCD für mehrere Bereiche konfigurieren. • Alle Vertrauensstellungen müssen bidirektionale, transitive Gesamtstruktur-Vertrauensstellungen sein. • Stellen Sie sicher, dass die Latenz zwischen den UEM Core-Instanzen und der Microsoft SQL Server-Datenbank maximal 5 ms beträgt. **Hinweis:** Wenn Sie ein Upgrade von der UEM-Version 12.19 oder früher auf UEM 12.20 oder höher durchführen, müssen Sie Folgendes durchführen: 1. Erstellen Sie eine neue Kerberos-Schlüsseltabellendatei und kopieren Sie sie auf jeden UEM-Server (siehe Schritt 2 in Konfigurieren von KCD für BlackBerry Dynamics-Apps). 2. Geben Sie unter Einstellungen > BlackBerry Dynamics > Eigenschaften im Feld „Dienstkontoname“, unter dem der KCD-Dienst ausgeführt wird (gc.krb5.principal.name) Folgendes an: `GCSvc/<UEM_Core_host_machine>`

Konfigurieren von KCD für BlackBerry Dynamics-Apps

Bevor Sie beginnen:

- Lesen Sie Voraussetzungen für die Konfiguration von KCD für BlackBerry Dynamics-Apps.
- Wenn Sie KCD für BlackBerry Docs konfigurieren, finden Sie weitere Informationen unter Konfigurieren der eingeschränkten Kerberos-Delegierung für den Docs-Dienst in der BlackBerry Enterprise Mobility Server-Dokumentation.

1. Um das Kerberos-Dienstkonto einer SPN auf dem Active Directory-Server zuzuordnen, öffnen Sie die Eingabeaufforderung als Administrator, und geben Sie Folgendes ein, wobei Sie den Namen des Hostservers, die Domäne und das Kerberos-Dienstkonto angeben. Das Kerberos-Dienstkonto ist der Name des Dienstkontos, unter dem der KCD-Dienst in UEM konfiguriert wird (gc.krb5.principal.name). Dieses Konto muss nicht mit dem UEM-Dienstkonto identisch sein, kann jedoch.

   ```
   setspn –s GCSvc/<UEM_Core_host_machine> <domain>\<Kerberos_service_account>
   ```

   Beispiel:

   ```
   setspn –s GCSvc/uem1.example.com example.com\kcdadmin
   ```

2. Führen Sie die folgenden Schritte aus, um eine neue Kerberos-Schlüsseltabellendatei zu erstellen und das Kennwort für das Kerberos-Konto festzulegen:
   a) Öffnen Sie auf dem KDC-Server eine Eingabeaufforderung.
   b) Führen Sie den folgenden Befehl aus, und geben Sie die entsprechenden Werte an:

   ```
   ktpass -out <output_filename>.keytab -mapuser
    <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> -princ
    <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> -ptype KRB5_NT_PRINCIPAL -
   pass <Kerberos_account_password>
   ```

Wenn Ihr Unternehmen eine Kerberos-Umgebung mit mehreren Bereichen im Einsatz hat, verwenden Sie stattdessen den folgenden Befehl:

```
ktpass -out <output_filename>.keytab -mapuser
 <Kerberos_service_account>@<KERBEROS_REALM_IN_UPPERCASE>
 -princ GCSvc/<UEM_Core_host_machine> -princ GCSvc/
<UEM_Core_host_machine>@<KERBEROS_REALM_IN_UPPERCASE> -ptype
 KRB5_NT_PRINCIPAL -pass <Kerberos_account_password>
```

c) Kopieren Sie die neue Schlüsseltabellendatei auf jeden UEM-Server, auf dem Sie dasselbe KCD-Administratorkonto verwenden möchten.

3. Erlauben Sie die Zählung der Gruppenmitgliedschaft von Active Directory-Benutzerobjekten. Weitere Informationen finden Sie unter Anhang B: Privilegierte Konten und Gruppen in Active Directory.
4. Führen Sie auf jedem UEM-Server die folgenden Schritte aus, um Berechtigungen für das UEM-Dienstkonto zu konfigurieren, damit es Benutzeranmeldeinformationen an das Kerberos-System senden kann (dies ist dasselbe Konto, das über die zugehörige SPN verfügt):
   a) Navigieren Sie in der Microsoft-Verwaltungskonsole zu **Lokale Sicherheitsrichtlinie > Lokale Richtlinien > Zuweisung von Benutzerrechten**.
   b) Öffnen Sie die Eigenschaften von **Als Teil des Betriebssystems agieren**, und klicken Sie auf **Benutzer oder Gruppe hinzufügen**.
   c) Geben Sie einen Namen für das Dienstkonto ein, und klicken Sie auf **OK**.
5. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Globale Eigenschaften**.
6. Aktivieren Sie das Kontrollkästchen **Explizites UPN verwenden**.
7. Aktivieren Sie das Kontrollkästchen **KCD aktivieren**.
8. Klicken Sie auf **Speichern**.
9. Klicken Sie in der Menüleiste auf **Einstellungen > BlackBerry Dynamics > Eigenschaften** und dann auf den Servernamen.
10. Geben Sie in das Feld **Vollständig qualifizierter Name für das KDC (gc.krb5.kdc)** den vollständig qualifizierten Namen für das KDC ein. Er entspricht in der Regel dem FQDN eines Active Directory-Domänen-Controllers.
11. Geben Sie im Feld **Speicherort der Schlüsseltabellendatei (gc.krb5.keytab.file)** den Speicherort der Schlüsseltabellendatei ein. Verwenden Sie Schrägstriche im Pfadnamen.
12. Geben Sie in das Feld **Dienstkontoname, unter dem der KDC-Dienst ausgeführt wird (gc.krb5.principal.name)** den Namen des Dienstkontos ein, das vom KCD-Dienst verwendet wird.

    Geben Sie in einer Kerberos-Umgebung mit mehreren Bereichen stattdessen Folgendes an:

    ```
    GCSvc/<UEM_Core_host_machine>
    ```

13. Geben Sie im Feld **Bereich – Active Directory (gc.krb5.realm)** den Namen des Active Directory-Bereichs in Großbuchstaben ein.
14. Geben Sie im Feld **Speicherort der krb5.config-Datei auf dem GC-Server (gc.krb5.config.file)** den Speicherort der krb5.config-Datei ein.

    Weitere Informationen zu den für die Datei krb5.conf geltenden Anforderungen finden Sie unter Voraussetzungen für die Konfiguration von KCD für BlackBerry Dynamics-Apps.
15. Klicken Sie auf **Speichern**.

Anforderungen zur Unterstützung von Kerberos PKINIT für BlackBerry Dynamics-Apps

BlackBerry UEM unterstützt Kerberos PKINIT für die BlackBerry Dynamics-Benutzerauthentifizierung mithilfe von PKI-Zertifikaten. Wenn Sie Kerberos PKINIT für BlackBerry Dynamics-Apps verwenden möchten, muss Ihre Organisation die folgenden Anforderungen erfüllen:

Objekt	Anforderungen
KDC	• Sie müssen den KDC-Host zur Liste der zulässigen Domänen im zugewiesenen BlackBerry Dynamics-Konnektivitätsprofil hinzufügen. Weitere Informationen finden Sie unter Erstellen eines BlackBerry Dynamics-Konnektivitätsprofils in der Dokumentation für Administratoren. • Der KDC-Host muss den TCP-Port 88 überwachen (der Kerberos-Standardport). • Das KDC muss einen A- (IPv4) oder AAAA-Datensatz (IPv6) in Ihrem DNS aufweisen. • BlackBerry Dynamics bietet keine Unterstützung für das KDC über UDP. • BlackBerry Dynamics verwendet keine Kerberos-Konfigurationsdateien (z. B. krb5.conf), um das richtige KDC zu suchen. • Das KDC kann den Client auf einen anderen KDC-Host verweisen. BlackBerry Dynamics folgt dem Verweis, solange der KDC-Host, auf den verwiesen wird, der Liste der zulässigen Domänen im BlackBerry Dynamics-Konnektivitätsprofil hinzugefügt wird. • Das KDC kann das TGT transparent in BlackBerry Dynamics von einem anderen KDC-Host abrufen. • Die eingeschränkte Kerberos-Delegierung darf nicht aktiviert sein.

Serverzertifikate	• Windows-KDC-Serverzertifikate, die über die Active Directory-Zertifikatdienste ausgegeben wurden, dürfen nur aus den folgenden Windows Server-Versionen stammen. Es werden keine anderen Serverversionen unterstützt.
	  • Internet Information Server mit Windows Server 2008 R2
	  • Internet Information Server mit Windows Server 2012 R2
	• Gültige KDC-Dienstzertifikate müssen sich entweder im BlackBerry Dynamics-Zertifikatspeicher oder im Gerätezertifikatspeicher befinden.

Client-Zertifikate	• Die minimale Schlüssellänge für die Zertifikate muss 2.048 Byte betragen. • Die Eigenschaft „Erweiterte Schlüsselnutzung“ des Zertifikats muss Microsoft Smart Card-Anmeldung (1.3.6.1.4.1.311.20.2.2) lauten. • Client-Zertifikate müssen den Benutzerprinzipalnamen (UPN; zum Beispiel user@domain.com) im alternativen Antragstellernamen der Objekt-ID „szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3“ enthalten. • Wenn dem Benutzer mehr als ein Client-Zertifikat ausgestellt wird, muss die Domäne des Benutzerprinzipalnamens mit der Domäne der Ressource übereinstimmen, auf die zugegriffen wird, um sicherzustellen, dass das richtige Zertifikat verwendet wird. • Zertifikate müssen gültig sein. Überprüfen Sie sie anhand der oben aufgeführten Server.

Verschlüsseln der Verbindung zwischen dem BlackBerry UEM und Microsoft SQL Server

Sie können eine verschlüsselte Verbindung zwischen dem BlackBerry UEM und Microsoft SQL Server konfigurieren. Standardmäßig ist die Verbindung nicht verschlüsselt.

Hinweis:

- Wenn Sie ein Upgrade eines UEM durchführen, werden die Einstellungen für die Verschlüsselung nicht beibehalten. Nach dem Upgrade müssen Sie Schritt 3 und folgende wiederholen, um die Verbindung erneut zu verschlüsseln.
- Bitte beachten Sie, dass die verschlüsselte Verbindung zu einer erhöhten Auslastung der UOS-CPU auf dem Computer führen kann, der den BlackBerry UEM Core hostet.

Bevor Sie beginnen:

- Verwenden Sie auf dem Computer, der den SQL Server hostet, in der Microsoft-Verwaltungskonsole das Zertifikat-Snap-in, um das Computerzertifikat anzufordern (wählen Sie das Computerkonto aus, danach Zertifikate (lokaler Computer) > klicken Sie mit der rechten Maustaste auf Persönlich > Alle Tasks > Neues Zertifikat anfordern). Das Zertifikat sollte unter Zertifikate (lokaler Computer) > Persönlich > Zertifikate angezeigt werden.
  Je nachdem, wie SQL Server konfiguriert ist, müssen Sie dem SQL Server-Konto möglicherweise Berechtigungen für das Zertifikat erteilen.
- Navigieren Sie im SQL Server-Konfigurationsmanager zur Netzwerkkonfiguration, und öffnen Sie die Eigenschaften für die SQL Server-Protokolle. Wählen Sie auf der Registerkarte „Zertifikat“ das Computerzertifikat aus. Starten Sie den SQL Server-Dienst neu.
- Verwenden Sie in der Microsoft-Verwaltungskonsole das Zertifikat-Snap-in, um das Computerzertifikat aus dem persönlichen Speicher (personal.cer) zu exportieren. Kopieren Sie das Zertifikat auf jeden Computer, der eine UEM-Instanz hostet.

Schließen Sie diesen Schritt auf jedem Computer ab, der eine UEM Core-Instanz hostet.

1. Navigieren Sie zum persönlichen Zertifikat (personal.cer) und doppelklicken Sie darauf. Zeigen Sie das übergeordnete Zertifikat (parent.cer) an, exportieren und speichern Sie es im selben Ordner, in dem sich das persönliche Zertifikat befindet (z. B. C:\blackbberry\certs\).
2. Öffnen Sie die Eingabeaufforderung und führen Sie die folgenden Befehle aus, um die persönlichen und übergeordneten Zertifikate in den Java-Keystore zu importieren und einen Truststore zu generieren:

```
keytool -importcert -keystore "<path_to_Java_CA_certs_store>" -
storepass <CA_certs_store_password> -file <path_to_personal_cert> -alias
 personal

keytool -importcert -keystore "<path_to_Java_CA_certs_store>" -
storepass <CA_certs_store_password> -file <path_to_parent_cert> -alias parent

keytool -import -v -trustcacerts -alias personal -file <path_to_personal_cert>
 -keystore <path_to_folder_with_personal_and_parent_certs>\truststore.jks -
storepass <password_to_set_for_trust_store> -storetype JKS
```

   Beispiel:

```
keytool -importcert -keystore "c:\Program Files\Eclipse Adoptium\jre-17.0.11.9-
hotspot\lib\security\cacerts" -storepass changeit -file c:\blackberry\certs
\personal.cer -alias personal
```

```
keytool -importcert -keystore "c:\Program Files\Eclipse Adoptium\jre-17.0.11.9-
hotspot\lib\security\cacerts" -storepass changeit -file c:\blackberry\certs
\parent.cer -alias parent

keytool -import -v -trustcacerts -alias personal -file c:\blackberry\certs
\personal.cer -keystore c:\blackberry\certs\truststore.jks -storepass password
 -storetype JKS
```

3. Beenden Sie alle UEM-Dienste.
4. Kopieren Sie unter C:\Program Files\BlackBerry\UEM\common-settings **db.properties** und benennen Sie es um, um eine Eigenschaftsdatei für die Sicherungsdatenbank zu erstellen.
5. Öffnen Sie **db.properties**.
6. Konfigurieren Sie im Abschnitt SQL Server-Verschlüsselungseinstellungen die folgenden Einstellungen (andere Einstellungen müssen nicht geändert werden):

```
configuration.database.ng.encrypt=true
configuration.database.ng.trustservercertificate=false
configuration.database.ng.truststore=<path_to_the_jks_trust_store_generated_in_step_2>
configuration.database.ng.truststorepassword=<password_for_jks_trust_store_generated_in_st
```

7. Speichern und schließen Sie **db.properties**.
8. Starten Sie die UEM-Dienste neu.

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 (lokal) herstellen, damit Cisco ISE auf Daten von Geräten zugreifen kann, die auf 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 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 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 Geräte sperren, geschäftliche oder alle Daten von Geräten löschen. Weitere Informationen zum Netzwerkzugriff und zur Gerätesteuerung finden Sie unter Verwalten von Netzwerkzugriff und Gerätesteuerelementen über Cisco ISE.

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

Schritt	Aktion
1	Stellen Sie sicher, dass die Umgebung Ihres Unternehmens die Anforderungen an die Vernetzung von UEM mit Cisco ISE erfüllt.
2	Verbinden Sie UEM mit Cisco ISE, und richten Sie ein Autorisierungsprofil und Zugriffsrichtlinien ein.

Verwalten von Netzwerkzugriff und Gerätesteuerelementen über Cisco ISE

Cisco Identity Services Engine (ISE) Administratoren können die folgenden Aktionen durchführen.

Aktion	Beschreibung
Anzeigen der Gerätedaten.	Sie können Informationen über die mit BlackBerry UEM verknüpften Geräte anzeigen, z. B.: • MAC-Adresse • Ob das Gerät mit UEM richtlinienkonform ist • ob Gerätedaten verschlüsselt sind • Ob das Gerät unter UEM aktiviert (registriert) ist • ob das Gerät gegen eine der Bedingungen für Richtlinientreue (z. B. im Hinblick auf Jailbreak oder Rooting) verstößt • 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 Zugriffsrichtlinie festlegen, die verhindert, dass Geräte, die nicht mit UEM richtlinienkonform sind, auf das Unternehmensnetzwerk zugreifen.
Sperren eines Geräts	Sperren Sie das Gerät eines Benutzers. Diese Funktion ist nützlich, wenn das Gerät eines Benutzers vorübergehend verlegt wurde. UEM sperrt das Gerät über einen IT-Administrationsbefehl. 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. UEM löscht geschäftliche Daten mithilfe eines IT-Administrationsbefehls. Gerätebenutzer können diese Aktion auch über das My Device portal ausführen.
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. UEM löscht alle Gerätedaten mithilfe eines IT-Administrationsbefehls. Gerätebenutzer können diese Aktion auch über das My Device portal ausführen.

Anforderungen: Integration von BlackBerry UEM und Cisco ISE

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

Objekt	Anforderungen
Unterstütztes Betriebssystem	Jedes Betriebssystem, das UEM unterstützt, mit Ausnahme von Windows 10 für Desktop.
Abhörport	Cisco ISE verwendet den standardmäßigen BlackBerry Web Services-Überwachungsport 18084, um Gerätedaten aus UEM abzurufen. Wenn Port 18084 bei der Installation von 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 UEM und Cisco ISE vorhanden ist, konfigurieren Sie die Firewall so, dass HTTPS-Sitzungen zwischen beiden Systemen zulässig sind.
Administratorkonto	Cisco ISE erfordert ein dediziertes 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 Die Standardrollen „Sicherheitsadministrator“ und „Unternehmensadministrator“ verfügen über diese Berechtigungen, oder Sie können eine benutzerdefinierte Rolle mit diesen Berechtigungen erstellen. Weitere Informationen finden Sie unter Erstellen eines Administrators in der Dokumentation für Administratoren.

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 UEM-Administratorkonto an einen UEM-Administrator. Die aktuelle Cisco ISE-Dokumentation finden Sie unter Cisco ISE Configuration Guide.

Bevor Sie beginnen: Navigieren Sie in einem Browser zu **https://<*server_name*>:<*BlackBerry_Web_Services_port*>/enterprise/admin/util/ws?wsdl**, wobei *<server_name>* der FQDN des Computers ist, der die BlackBerry UEM Core-Komponente hostet. Der *<BlackBerry_Web_Services_port>*-Standardwert ist 18084. Exportieren Sie das BlackBerry Web Services-Zertifikat über Ihren Browser, und speichern Sie es auf Ihrem Desktop.

1. Melden Sie sich bei der Cisco ISE-Verwaltungskonsole an.
2. Importieren Sie das BlackBerry Web Services-Zertifikat in den Cisco ISE-Speicher für vertrauenswürdige Zertifikate. Wählen Sie die Optionen aus, die für die Client-Authentifizierung und Syslog sowie für die Authentifizierung von Cisco-Diensten vertrauenswürdig sind.
3. Fügen Sie einen externen MDM-Dienst hinzu, und geben Sie die Details der UEM-Instanz an, einschließlich des FQDN oder der IP-Adresse der UEM-Domäne, des Ports (Standard 18084) und der Anmeldeinformationen des UEM-Administratorkontos.

4. Geben Sie für das Abfrageintervall ein, wie oft (in Minuten) Cisco ISE Gerätedaten von UEM abrufen soll. Es wird empfohlen, den Standardwert zu verwenden.

   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 UEM ab.
5. Bearbeiten und testen Sie die Verbindung zu UEM.

Nachdem die Verbindung hergestellt wurde, können Sie die Verzeichnisattribute für UEM in der Cisco ISE-Verwaltungskonsole anzeigen. 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.

- Konfigurieren Sie ACLs auf dem Wireless-LAN-Controller.
- Konfigurieren Sie ein Autorisierungsprofil, das Geräte zur BlackBerry UEM Self-Service-Konsole umleitet, wenn sie versuchen, auf das geschäftliche Netzwerk zuzugreifen, während das Gerät unter UEM nicht aktiviert ist. Der Benutzer benötigt ein 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 UEM-Administrator wenden müssen, wenn sie von Cisco ISE auf die Anmeldungsseite umgeleitet werden.
- Konfigurieren Sie Richtlinienregeln für die Autorisierung, die bestimmen, wie Cisco ISE Geräte verarbeitet, die nicht unter UEM aktiviert wurden oder nicht mit UEM konform sind.

Einrichten eines VPN mit Knox StrongSwan für UEM-Dark-Site-Umgebungen

In einer UEM-Dark-Site-Umgebung müssen Sie den VPN-Zugriff auf Ihre Umgebung einrichten, damit Samsung Knox-Geräte auf Ihre internen Server und Ressourcen zugreifen können. Weitere Informationen zu UEM-Dark-Site-Umgebungen finden Sie unter Installation und Upgrade von BlackBerry UEM in einer Dark-Site-Umgebung in der Dokumentation zur Installation.

Bevor Sie beginnen: Laden Sie das Knox Service Plugin und die Android VPN Management für Knox StrongSwan-Apps herunter, und fügen Sie die APK-Dateien dem freigegebenen Netzwerkspeicherort für interne Apps hinzu.

1. Fügen Sie das Knox Service Plugin und die Android VPN Management für Knox StrongSwan-Apps der App-Liste hinzu.
2. Wählen Sie die Knox Service Plugin-App aus, und klicken Sie auf +, um die Konfigurationsoptionen für die App festzulegen.
   a) Wählen Sie unter **VPN-Profil** die Option **Integriertes Knox-VPN** aus.
   b) Legen Sie unter **Parameter für Integriertes Knox-VPN (für StrongSwan)** die folgenden Optionen fest:
      - Legen Sie den **Authentifizierungstyp** auf "ipsec_ike2_rsa“ fest.
      - Legen Sie den **Alias für das Benutzerzertifikat** als Benutzername mit Anhang „_1 [Knox]“ fest. Sie können Variablen für den Benutzernamen verwenden (z. B. `%UserFirstName% %UserLastName% _1 [Knox]`).
      - Legen Sie den **Alias für Zertifizierungsstellenzertifikat** als Benutzername mit Anhang „ [Knox]“ fest. Sie können Variablen für den Benutzernamen verwenden (z. B. `%UserFirstName% %UserLastName% [Knox]`).
3. Weisen Sie die App dem Benutzer zu.
4. Erstellen Sie ein Profil für Zertifizierungsstellenzertifikate, um das VPN-Serverzertifikat an Geräte zu senden und Benutzern zuzuweisen.
5. Fügen Sie ein VPN-Clientzertifikat für jeden Benutzer hinzu.

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada