BlackBerry UEM Cloud

Konfigurationshandbuch

Inhalt

Erstmalige Konfiguration von BlackBerry UEM Cloud

In der folgenden Tabelle sind die Konfigurationsaufgaben, die in diesem Handbuch besprochen werden, zusammengefasst. Diese Aufgaben sind je nach Unternehmensanforderungen optional. Verwenden Sie diese Tabelle, um zu bestimmen, welche Konfigurationsaufgaben Sie abschließen sollten.

Nach Abschluss der entsprechenden Aufgaben sind Sie bereit, Administratoren und Gerätekontrollen einzurichten, Benutzer und Gruppen zu erstellen und Geräte zu aktivieren.

Aufgabe	Beschreibung
Verbinden mit dem lokalen Firmenverzeichnis Ihres Unternehmens und Aktivieren der Sicherheits- und Konnektivitätsfunktionen	Sie können BlackBerry Connectivity Node installieren, aktivieren und konfigurieren, um den Zugriff auf das lokale Firmenverzeichnis Ihres Unternehmens zu ermöglichen und Sicherheits- und Konnektivitätsfunktionen zu aktivieren.
Konfigurieren von BlackBerry Connectivity Node zum Senden von Daten über einen Proxy-Server	Sie können die BlackBerry Connectivity Node-Komponenten zum Senden von Daten über einen Proxy-Server in der Umgebung Ihres Unternehmens konfigurieren.
Verbinden von BlackBerry UEM mit Microsoft Azure	Wenn Sie BlackBerry UEM mit Azure Active Directory verbinden möchten, verwenden Sie BlackBerry UEM für die Bereitstellung von iOS- und Android-Apps, die von Microsoft Intune verwaltet werden, oder verwalten Sie Windows 10-Apps in BlackBerry UEM, und verbinden Sie BlackBerry UEM mit Microsoft Azure.
Verknüpfen von Unternehmensverzeichnisgruppen mit BlackBerry UEM-Gruppen	Wenn Sie BlackBerry UEM mit Ihrem Unternehmensverzeichnis verbinden, können Sie per Verzeichnis verknüpfte Gruppen aktivieren, um das Onboarding und die Verwaltung von Benutzern zu vereinfachen.
APNs-Zertifikat abrufen und registrieren	Wenn Sie iOS- oder macOS-Geräte verwalten und Daten an diese Geräte senden möchten, müssen Sie eine signierte CSR-Datei von BlackBerry abrufen, mit dieser ein APNs-Zertifikat von Apple abrufen und das APNs-Zertifikat bei der BlackBerry UEM-Domäne registrieren.
Konfigurieren von BlackBerry UEM für die Unterstützung von Android-Geräten, die ein Arbeitsprofil besitzen	Zur Unterstützung von Android-Geräten, die ein Arbeitsprofil haben, müssen Sie Ihre G Suite- oder die Google Cloud-Domäne zur Unterstützung von Mobilgerätemanagementlösungen von Drittanbietern und BlackBerry UEM für die Kommunikation mit Ihrer G Suite- oder Google Cloud-Domäne konfigurieren.
Konfigurieren von BlackBerry UEM für das Programm zur Geräteregistrierung von Apple	Wenn Sie die BlackBerry UEM-Verwaltungskonsole zum Verwalten der iOS-Geräte verwenden möchten, die von Ihrem Unternehmen von Apple für das Programm zur Geräteregistrierung (DEP) erworben wurden, müssen Sie diese Funktion konfigurieren.
Konfigurieren von BlackBerry UEM Cloud für die Unterstützung von BlackBerry Dynamics-Apps	Wenn Sie Benutzern gestatten möchten, BlackBerry Dynamics-Apps zu verwenden, können Sie BlackBerry UEM Cloud zur Unterstützung der Apps einrichten.

Aufgabe	Beschreibung
Migrieren von Benutzern, Gruppen und anderen Daten aus BlackBerry UEM	Über die Verwaltungskonsole können Sie Benutzer, Geräte, Gruppen und andere Daten aus einer lokalen BES12-oder einer BlackBerry UEM-Datenbank migrieren.

Zur Konfiguration von BlackBerry UEM erforderliche Administratorberechtigungen

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

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

Abrufen und Aktivieren von Lizenzen

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

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

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 BlackBerry UEM Cloud den Zugriff auf das lokale Firmenverzeichnis des Unternehmens. Sie können Verzeichnisbenutzerkonten erstellen, indem Sie nach Benutzerdaten im Unternehmensverzeichnis suchen und diese importieren. Benutzerdaten werden täglich mit dem Verzeichnis synchronisiert. BlackBerry 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.
BlackBerry Proxy	BlackBerry Proxy hält eine sichere Verbindung zwischen Ihrem Unternehmen und BlackBerry Dynamics NOC aufrecht, die BlackBerry Dynamics-Apps eine sichere Kommunikation mit den Ressourcen Ihres Unternehmens hinter der Firewall erlaubt. Er unterstützt zudem BlackBerry Dynamics Direct Connect, eine Komponente, die App-Daten das Umgehen von BlackBerry Dynamics NOC ermöglicht. Weitere Informationen finden Sie unter Konfiguration von BlackBerry UEM Cloud für die Unterstützung von 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 in der Dokumentation für Administratoren
BlackBerry Secure Gateway	Der 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 in der Dokumentation für Administratoren
BlackBerry Gatekeeping Service	Der BlackBerry Gatekeeping Service erleichtert die Steuerung der Geräte, die auf Exchange ActiveSync zugreifen können. Weitere Informationen finden Sie in der Dokumentation für Administratoren

Die Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node sind in der Verwaltungskonsole vorhanden. Sie können diese Dateien zur Installation neuer Instanzen des BlackBerry Connectivity Node und für Upgrades vorhandener Instanzen verwenden. Sie müssen vorhandene Instanzen des BlackBerry Connectivity Node nach der Einführung einer neuen Version von BlackBerry UEM Cloud aktualisieren.

BlackBerry Connectivity Node-Planungsinformationen

Bevor Sie BlackBerry Connectivity Node installieren, beachten Sie die folgenden Informationen.

Hardware

Der BlackBerry Connectivity Node muss auf einem für technische Zwecke reservierten, dedizierten Computer installiert werden, 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 den BlackBerry Connectivity Node nicht auf einem Computer installieren, der bereits eine lokale BlackBerry UEM-Instanz hostet.

- 4 Prozessorkerne, 2,7 GHz
- 8 GB verfügbarer Arbeitsspeicher
- 64 GB Festplattenspeicher
- Überprüfen Sie, ob der Computer, der den BlackBerry Connectivity Node hostet, die folgenden Mindestanforderungen an die Hardware erfüllt:

Software

Um zu überprüfen, ob Ihre Umgebung die Anforderungen an die Installation des BlackBerry Connectivity Node erfüllt, sehen Sie sich die Kompatibilitätsmatrix an.

Skalierbarkeit und hohe Verfügbarkeit

Jeder BlackBerry Connectivity Node kann bis zu 5000 Geräte unterstützen. Sie können weitere BlackBerry Connectivity Node s installieren, um bis zu 50.000 weitere Geräte zu unterstützen.

Sie können drei oder mehr Instanzen des BlackBerry Connectivity Node installieren, um Redundanz zu bieten. Sie müssen jede Instanz auf einem dedizierten Computer installieren. Verwenden Sie für alle Instanzen dieselbe Unternehmensverzeichniskonfiguration.

Durch die Bereitstellung von mehr als einem BlackBerry Connectivity Node in einer Servergruppe wird eine hohe Verfügbarkeit und Lastverteilung erzielt.

Schritte zum Installieren und Aktivieren von BlackBerry Connectivity Node

Führen Sie zum Installieren und Aktivieren von BlackBerry Connectivity Node die folgenden Schritte durch:

1	Stellen Sie sicher, dass Ihr Unternehmen die Voraussetzungen für die Installation von BlackBerry Connectivity Node erfüllt.
2	Laden Sie die Installations- und die Aktivierungsdateien für BlackBerry Connectivity Node über die Verwaltungskonsole herunter.

3	Installieren, Aktivieren und Konfigurieren Sie BlackBerry Connectivity Node.
4	Konfigurieren Sie bei Bedarf die Proxy-Einstellungen für die BlackBerry Connectivity Node-Komponenten.
5	Führen Sie weitere Konfigurationsschritte für BlackBerry Secure Connect Plus, den BlackBerry Secure Gateway, den BlackBerry Gatekeeping Service und die BlackBerry Dynamics-Apps durch.

Voraussetzungen: Installation von BlackBerry Connectivity Node

- Überprüfen Sie, ob Windows PowerShell 2.0 oder höher auf dem Computer ausgeführt wird. Dies ist erforderlich, damit die Setup-Anwendung RRAS für BlackBerry Secure Connect Plus und den BlackBerry Gatekeeping Service installieren kann.

  Hinweis: Sollte die Setupanwendung RRAS nicht auf Ihrem Computer installieren können, müssen Sie die Installation anhalten, RRAS manuell installieren und die Installation neu starten.
- Wählen Sie ein Verzeichniskonto mit Leseberechtigung, dass der BlackBerry Cloud Connector für den Zugriff auf das Unternehmensverzeichnis verwenden kann.
- Verwenden Sie ein BlackBerry UEM Cloud-Konto mit Berechtigungen zum Herunterladen der BlackBerry Connectivity Node-Installations- und -Aktivierungsdateien (z. B. Sicherheitsadministratorkonto).
- Verwenden Sie ein Windows-Konto mit Berechtigungen zum Installieren und Konfigurieren der Software auf dem Computer, der den BlackBerry Connectivity Node hostet.
- 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

Installation oder Upgrade des BlackBerry Connectivity Node

Befolgen Sie die Anweisungen in diesem Abschnitt zur Installation oder zum Durchführen eines Upgrades von BlackBerry Connectivity Node.

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

Sie müssen jede Instanz auf einem dedizierten Computer installieren. Verwenden Sie für alle Instanzen dieselbe Unternehmensverzeichniskonfiguration.

Herunterladen der Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node

1. Klicken Sie in der Menüleiste der Verwaltungskonsole 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 Sie das Installationspaket.

5. 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.
6. Klicken Sie auf **Erstellen**.
7. Speichern Sie die Aktivierungsdatei (.txt).

   Die Aktivierungsdatei ist 60 Minuten lang gültig. Wenn Sie die Aktivierungsdatei nicht innerhalb von 60 Minuten verwenden, müssen Sie eine neue Aktivierungsdatei generieren. Nur die letzte Aktivierungsdatei ist gültig.

Wenn Sie fertig sind: Installieren und Konfigurieren von BlackBerry Connectivity Node.

Installieren und Konfigurieren von BlackBerry Connectivity Node

Bevor Sie beginnen: Herunterladen der Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node .

1. Öffnen Sie die BlackBerry Connectivity Node-Installationsdatei (.exe), die Sie über die Verwaltungskonsole heruntergeladen haben.

   Wenn eine Windows-Meldung mit dem Hinweis angezeigt wird, dass eine Erlaubnis für das Vornehmen von Änderungen am Computer benötigt wird, klicken Sie auf **Ja**.
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 BlackBerry Connectivity Node aktivieren, werden Daten über Port 443 (HTTPS) an die BlackBerry Infrastructure (<*Region*>.bbsecure.com) gesendet. Nach der Aktivierung verwendet BlackBerry Connectivity Node Port 3101 (TCP) für alle ausgehenden Verbindungen über die BlackBerry Infrastructure. Wenn Sie Daten von 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 „<*Region*>.bbsecure.com“ senden können. Klicken Sie auf **Speichern**.
   - Um andere ausgehende Verbindungen von den Komponenten von 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 „<*Region*>.bbsecure.com“ senden können. Klicken Sie auf **Speichern**.
10. Geben Sie im Feld **Anzeigename** einen Namen für BlackBerry Connectivity Node ein. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Durchsuchen**. Wählen Sie die Aktivierungsdatei aus, die Sie über die Verwaltungskonsole heruntergeladen haben.
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 (<*Region*>.bbsecure.com) zur Aktivierung von BlackBerry Connectivity Node und zur selben bbsecure.com-Region wie die Hauptinstanz von BlackBerry Connectivity Node zulassen.

13. Klicken Sie in der Dropdown-Liste auf den von Ihrem Unternehmen verwendeten Unternehmensverzeichnistyp.
14. Klicken Sie auf **Konfigurieren**.
15. Folgen Sie den Schritten für den Verzeichnistyp Ihres Unternehmens:

Verzeichnistyp	Schritte
Microsoft Active Directory	**a.** Geben Sie im Feld **Benutzername** den Benutzernamen für das Microsoft Active Directory-Konto ein. **b.** Geben Sie im Feld **Domäne** den FQDN der Domäne ein, die Microsoft Active Directory hostet. Beispiel: domain.example.com. **c.** Geben Sie im Feld **Kennwort** das Kennwort für das Microsoft Active Directory-Konto ein. **d.** 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. **e.** 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. **f.** 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. **g.** Wenn Sie die Unterstützung für verknüpfte Microsoft Exchange-Postfächer aktivieren möchten, klicken Sie in der Dropdown-Liste **Unterstützung für verknüpfte Microsoft Exchange-Postfächer** auf **Ja**. Um das Microsoft Active Directory-Konto für jede Gesamtstruktur zu konfigurieren, auf die BlackBerry UEM 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. **h.** Klicken Sie auf **Speichern**.

Verzeichnistyp	Schritte
LDAP-Verzeichnis	**a.** 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. **b.** 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. **c.** Geben Sie im Portfeld **LDAP** die Portnummer des LDAP-Computers ein. **d.** Wählen Sie in der Dropdown-Liste **Autorisierung erforderlich** aus, ob BlackBerry 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). **e.** Geben Sie im Feld **Basissuche** die Basissuche ein, auf die Sie zugreifen möchten (beispielsweise: OU=Users,DC=example,DC=com). **f.** 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)). **g.** Klicken Sie in der Dropdown-Liste **LDAP-Benutzersuchbereich** auf eine der folgenden Optionen: • Wenn Sie möchten, dass in der Benutzersuche alle Ebenen unter der Basis-DN durchsucht werden, klicken Sie auf **Alle Ebenen**. • Wenn Sie die Benutzersuche auf eine Ebene unter der Basis-DN beschränken möchten, klicken Sie auf **Eine Ebene**. **h.** 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. **i.** Geben Sie im Feld **Vorname** das Attribut für den Vornamen der einzelnen Benutzer ein (beispielsweise: givenName). **j.** Geben Sie im Feld **Nachname** das Attribut für den Nachnamen der einzelnen Benutzer ein (beispielsweise: sn). **k.** 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. **l.** Geben Sie im Feld **E-Mail-Adresse** das Attribut für die E-Mail der einzelnen Benutzer ein (beispielsweise: mail). **m.** Geben Sie im Feld **Anzeigename** das Attribut für den Anzeigenamen der einzelnen Benutzer ein (beispielsweise displayName). **n.** Wenn per Verzeichnis verknüpfte Gruppen aktiviert werden sollen, aktivieren Sie das Kontrollkästchen **Aktivieren von per Verzeichnis verknüpften Gruppen**. Weitere Informationen zu per Verzeichnis verknüpften Gruppen finden Sie unter Verknüpfen von Unternehmensverzeichnisgruppen mit BlackBerry UEM-Gruppen. **o.** Klicken Sie auf **Speichern**.

16. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup**.
17. 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 eine zweite BlackBerry Connectivity Node-Instanz als Redundanz zu installieren, laden Sie einen weiteren Satz Installations- und Aktivierungsdateien herunter, und wiederholen Sie diese Aufgabe auf einem anderen Computer. Verwenden Sie die gleiche Verzeichniskonfiguration. Dies sollte durchgeführt werden, nachdem die erste Instanz aktiviert wurde.
- Konfigurieren Sie ggf. die Proxy-Einstellungen für BlackBerry Connectivity Node. Anweisungen finden Sie unter Konfigurieren von BlackBerry Connectivity Node zur Verwendung des BlackBerry Router oder eines TCP-Proxy-Servers.
- Klicken Sie zum Ändern der konfigurierten Verzeichniseinstellungen in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Firmenverzeichnis**. Klicken Sie auf ✎ für die Verzeichnisverbindung.
- Wenn Sie Daten über einen HTTP-Proxy senden möchten, bevor diese BlackBerry Dynamics NOC erreichen, klicken Sie in der BlackBerry Connectivity Node-Konsole (http://localhost:8088) auf **Allgemeine Einstellungen > BlackBerry Router und Proxy**. Wählen Sie das Kontrollkästchen **HTTP-Proxy aktivieren** aus, und konfigurieren Sie die Proxyeinstellungen.
- 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 „Schützen von E-Mail-Daten mithilfe von BlackBerry Secure Gateway“ 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..

Ändern der Standardeinstellungen für BlackBerry Connectivity Node-Instanzen

Standardmäßig ist der BlackBerry Gatekeeping Service in jeder BlackBerry Connectivity Node-Instanz aktiv. Wenn Gatekeeping-Daten nur von dem BlackBerry Gatekeeping Service verwaltet werden sollen, der mit den primären BlackBerry UEM-Komponenten installiert wurde, können Sie die Standardeinstellungen ändern, um den BlackBerry Gatekeeping Service in jeder Instanz zu deaktivieren. Sie können auch die Standardeinstellungen für die Protokollierung aller BlackBerry Connectivity Node-Instanzen festlegen.

Die Standardeinstellungen gelten für jede BlackBerry Connectivity Node-Instanz, die sich nicht in der einer Servergruppe befindet. Wenn eine Instanz Teil einer Servergruppe ist, verwendet sie die für diese Servergruppe konfigurierten Standardeinstellungen.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup**.
2. Klicken Sie auf ⚙.
3. Wenn Sie den BlackBerry Gatekeeping Service in der jeweiligen Instanz deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Einstellungen des BlackBerry Gatekeeping Service überschreiben**.
4. Wenn Sie die Protokollierungseinstellungen konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Protokollierungseinstellungen überschreiben**. Führen Sie eine der folgenden Aufgaben 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 Höchstgrenzen für Größe und Alter der Protokolldateien festlegen möchten, aktivieren Sie das Kontrollkästchen **Lokalen Speicherpfad aktivieren**. Geben Sie die Größenbeschränkung (in MB) und die Altersbeschränkung (in Tagen) ein.

5. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Wenn Sie die BlackBerry Gatekeeping Service-Instanzen deaktiviert haben und sie erneut aktivieren möchten, aktivieren Sie das Kontrollkästchen **BlackBerry Gatekeeping Service aktivieren**. Jede Instanz muss in der Lage sein, auf den Gatekeeping-Server Ihres Unternehmens zuzugreifen.

Aktualisieren von BlackBerry Connectivity Node

Wenn Sie über ein Update für BlackBerry UEM Cloud benachrichtigt werden, gehen Sie gemäß den folgenden Anweisungen vor, um die BlackBerry Connectivity Node-Komponenten auf die neueste Version zu aktualisieren.

1. Öffnen Sie auf dem Computer, auf dem der BlackBerry Connectivity Node gehostet wird, die BlackBerry Connectivity Node-Konsole (http:/localhost:8088).
2. Notieren Sie die aktuellen Verzeichniskonfigurationseinstellungen.
3. Melden Sie sich bei der BlackBerry UEM Cloud-Verwaltungskonsole an.
4. Laden Sie die BlackBerry Connectivity Node-Installations- und Aktivierungsdateien herunter. Anweisungen finden Sie unter Herunterladen der Installations- und Aktivierungsdateien für den BlackBerry Connectivity Node.
5. Installieren und Konfigurieren von BlackBerry Cloud Connector mit den Informationen, die Sie in Schritt 2 notiert haben. Anweisungen finden Sie unter Installieren und Konfigurieren von BlackBerry Connectivity Node.

Erstellen von Servergruppen

Sie können regionale Verbindungen für Unternehmensverbindungsfunktionen einrichten, indem Sie BlackBerry Connectivity Node-Instanzen in einer bestimmten Region bereitstellen. Dies wird auch als Servergruppe bezeichnet.

Beim Erstellen einer Servergruppe geben Sie den regionalen Datenpfad an, den die zu verwendenden Komponenten für die Verbindung mit der BlackBerry Infrastructure nutzen sollen. Sie können E-Mail- und Enterprise-Konnektivitätsprofile mit einer Servergruppe verknüpfen. Jedes Gerät, dem diese Profile zugewiesen wurden, nutzt die regionale Verbindung dieser Servergruppe zur BlackBerry Infrastructure, wenn Komponenten der BlackBerry Connectivity Node verwendet werden.

Durch die Bereitstellung von mehr als einem BlackBerry Connectivity Node in einer Servergruppe wird eine hohe Verfügbarkeit und Lastverteilung erzielt.

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

Erstellen einer Servergruppe

Bevor Sie beginnen: Installieren eines zusätzlichen BlackBerry Connectivity Node

1. Klicken Sie in der Menüleiste 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. Wählen Sie in der Dropdown-Liste **Land** das Land aus, für das die Instanzen von BlackBerry Connectivity Node installiert werden sollen. Die der Servergruppe hinzugefügten BlackBerry Connectivity Node-Instanzen verwenden die regionale Verbindung zur BlackBerry Infrastructure des ausgewählten Landes.

   Hinweis: Sie können diese Einstellung nach dem Erstellen der Servergruppe nicht mehr ändern.

5. Standardmäßig muss jede BlackBerry Connectivity Node-Instanz mit demselben Unternehmensverzeichnis konfiguriert sein. Wenn Sie den Unternehmensverzeichnis-Connector für die BlackBerry Connectivity Node-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 unter **Einstellungen > Infrastruktur > BlackBerry Secure Connect Plus** konfigurierten Standardeinstellungen verwendet werden sollen, aktivieren Sie das Kontrollkästchen **DNS-Server überschreiben**. Führen Sie folgende Aufgaben aus:
   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.

   Weitere Informationen finden Sie unter „Verwenden von BlackBerry Secure Connect Plus für Verbindungen mit geschäftlichen Ressourcen“ in der Dokumentation für Administratoren.
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 Aufgaben 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 Höchstgrenzen für Größe und Alter der Protokolldateien festlegen möchten, aktivieren Sie das Kontrollkästchen **Lokalen Speicherpfad aktivieren**. Geben Sie die Größenbeschränkung (in MB) und die Altersbeschränkung (in Tagen) ein.
9. Wenn Sie den BlackBerry Connectivity Node nur für einen Verbindungstyp festlegen möchten, aktivieren Sie das Kontrollkästchen **Leistungsmodus für einzelnen Dienst aktivieren**. Wählen Sie im Dropdown-Menü den Verbindungstyp aus (**Nur BlackBerry Secure Connect Plus**, **Nur BlackBerry Secure Gateway** oder **Nur BlackBerry Proxy**.
10. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Wenn die BlackBerry Gatekeeping Service-Instanzen in einer Servergruppe deaktiviert wurden und erneut aktiviert werden sollen, wählen Sie die Servergruppe unter **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup** aus, und aktivieren Sie das Kontrollkästchen **BlackBerry Gatekeeping Service aktivieren**. Jede Instanz muss in der Lage sein, auf den Gatekeeping-Server Ihres Unternehmens zuzugreifen.
- Installieren und Konfigurieren Sie den BlackBerry Connectivity Node, und fügen Sie dann die Instanz zu einer Servergruppe hinzu.

Verwalten von Servergruppen

BlackBerry Connectivity Node-Instanzen können jederzeit zu einer Servergruppe hinzugefügt oder aus einer Servergruppe entfernt werden. Wenn Sie eine Instanz zu einer Servergruppe hinzufügen, verwendet diese Instanz die Einstellungen, die für diese Servergruppe definiert wurden (die Komponenten der Instanz verwenden z. B. die angegebene regionale Verbindung zur BlackBerry Infrastructure). Wenn Sie eine Instanz aus einer Servergruppe entfernen, verwendet diese Instanz die Standardeinstellungen, die auf dem BlackBerry Connectivity Node-Setupbildschirm definiert wurden (siehe Ändern der Standardeinstellungen für BlackBerry Connectivity Node-Instanzen).

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Connectivity Node Setup**.
2. Wählen Sie eine BlackBerry Connectivity Node-Instanz.
3. Führen Sie eine der folgenden Aufgaben aus:
   a) Um eine Instanz zu einer Servergruppe hinzuzufügen, klicken Sie auf . Wählen Sie die entsprechende Servergruppe aus. Klicken Sie auf **OK**.
   b) Um eine Instanz aus einer Servergruppe zu entfernen, klicken Sie auf . Klicken Sie im Bestätigungsdialogfeld auf **OK**.

Fehlerbehebung bei Problemen mit BlackBerry Connectivity Node

Beachten Sie bei der Fehlerbehebung im Zusammenhang mit BlackBerry Connectivity Node folgende gängige Probleme.

Weitere Informationen zu BlackBerry-Supportprogrammen finden Sie unter Technischer Support von BlackBerry.

Keine gleichzeitige Aktivierung von BlackBerry Connectivity Node und BlackBerry UEM Cloud

Beschreibung

Nachdem Sie die Aktivierungsdatei hochgeladen und auf „Aktivieren“ geklickt haben, wird in einer Fehlermeldung angezeigt, dass die Aktivierung nicht erfolgreich war.

Mögliche Lösungen

Führen Sie eine der folgenden Aktionen aus:

- Überprüfen Sie, ob die letzte Aktivierungsdatei, die Sie in der Verwaltungskonsole erstellt haben, hochgeladen wurde. Nur die letzte Aktivierungsdatei ist gültig.
- Aktivierungsdateien laufen nach 60 Minuten ab. Erstellen Sie eine neue Aktivierungsdatei, laden Sie sie hoch und führen Sie den Aktivierungsvorgang erneut durch.
- Gehen Sie zu http://support.blackberry.com/kb, um Artikel KB38964 zu lesen.

Keine Verbindung zwischen BlackBerry Connectivity Node und dem Unternehmensverzeichnis

Beschreibung

Nachdem Sie die Informationen für Ihr Unternehmensverzeichnis angegeben und auf „Speichern“ geklickt haben, wird in einer Fehlermeldung angezeigt, dass keine Verbindung zwischen dem BlackBerry Connectivity Node und dem Unternehmensverzeichnis hergestellt werden konnte.

Mögliche Lösungen

Führen Sie eine der folgenden Aktionen aus:

- Überprüfen Sie, ob die Einstellungen für das Unternehmensverzeichnis korrekt 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 für den BlackBerry Connectivity Node unter *<Laufwerk:>*:\Programme\BlackBerry \BlackBerry Connectivity Node\Logs.
- Wenn Sie Microsoft Active Directory verwenden, gehen Sie zu http://support.blackberry.com/kb, um Artikel KB36955 zu lesen.

Keine Verbindung zwischen BlackBerry Connectivity Node und BlackBerry UEM Cloud

Beschreibung

Beim Überprüfen der Verbindung zwischen BlackBerry Connectivity Node und BlackBerry UEM Cloud wird in einer Fehlermeldung angezeigt, dass die Überprüfung fehlgeschlagen ist.

Mögliche Lösungen

Führen Sie eine der folgenden Aktionen aus:

- 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 BlackBerry UEM Cloud nicht möglich ist. Standardmäßig befinden sich die Protokolldateien für den BlackBerry Cloud Connector unter *<Laufwerk:>*:\Programme\BlackBerry \BlackBerry Connectivity Node\Logs.

Die Liste mit BlackBerry Connectivity Node-Instanzen wird in der Verwaltungskonsole nicht geladen

Beschreibung

Beim Versuch, eine Liste der BlackBerry Connectivity Node-Instanzen in der Verwaltungskonsole zu laden, wird die Meldung „Wird geladen ...“ angezeigt, die Liste der Instanzen wird jedoch nicht angezeigt.

Mögliche Lösung

Gehen Sie zu http://support.blackberry.com/kb, um Artikel KB38878 zu lesen.

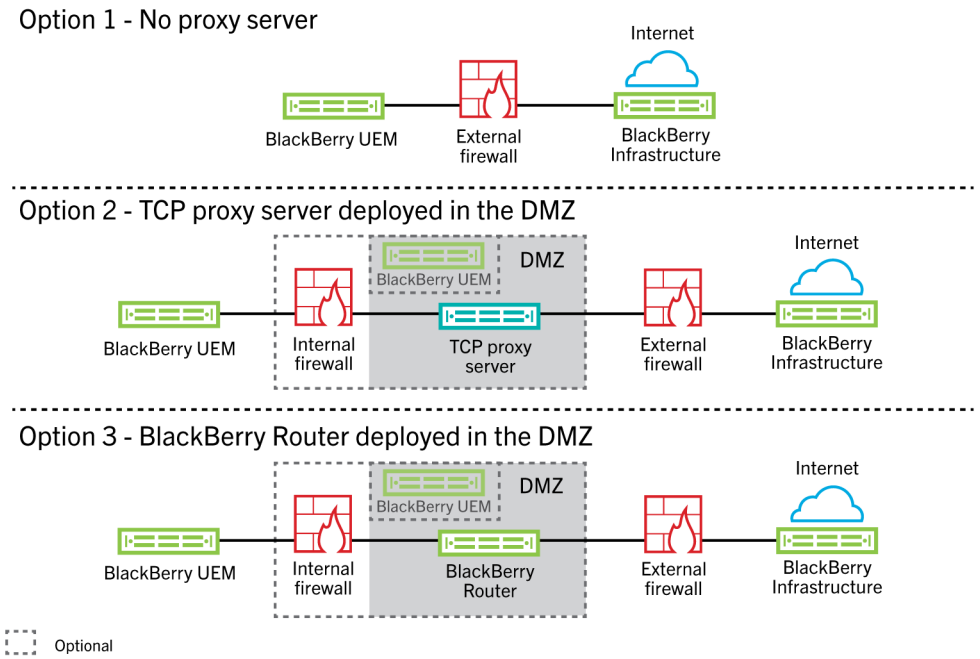
Konfigurieren von BlackBerry Connectivity Node zur Verwendung des BlackBerry Router oder eines TCP-Proxy-Servers

Um einen Proxy-Server mit BlackBerry Connectivity Node zu verwenden, können Sie den BlackBerry Router als Proxy-Server installieren oder einen bereits in der Umgebung Ihres Unternehmens installierten TCP-Proxy-Server verwenden.

Sie können den BlackBerry Router oder einen Proxy-Server außerhalb der Unternehmens-Firewall in einer DMZ installieren. Durch die Installation des BlackBerry Router oder eines TCP-Proxy-Servers in einer DMZ wird die Sicherheit zusätzlich erhöht. Nur der BlackBerry Router oder der Proxy-Server stellen 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 BlackBerry Router oder den Proxy-Server 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-Proxy-Server installieren. Der BlackBerry Router bzw. der TCP-Proxy-Server fungiert als Vermittler zwischen BlackBerry Connectivity Node und der BlackBerry Infrastructure.

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



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

Wenn Sie den BlackBerry Connectivity Node aktivieren, sendet dieser Daten über Port 443 (HTTPS) für die Aktivierung mit BlackBerry UEM Cloud. 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 BlackBerry UEM festlegen. Mehrere TCP-Proxy-Server mit SOCKS v5-Konfiguration (keine Authentifizierung) können Unterstützung bereitstellen, wenn eine der aktiven Proxy-Serverinstanzen nicht ordnungsgemäß funktioniert.

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

Vergleichen von TCP-Proxys

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

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

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

1. Klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Proxy**.
2. Wählen Sie die Option **Proxy-Server**.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Weiterleiten von HTTPS-Aktivierungsdaten für den BlackBerry Connectivity Node über einen Proxy-Server.	Geben Sie in den Feldern **Anmeldungs-Proxy** den FQDN oder die IP-Adresse und die Portnummer des Proxy-Servers ein. Der Proxy-Server muss Daten über Port 443 an „<*Region*>.bbsecure.com“ senden können.
Weiterleiten von ausgehenden Verbindungen von den Komponenten des BlackBerry Connectivity Node über einen Proxy-Server.	Geben Sie in den entsprechenden Feldern den FQDN oder die IP-Adresse und die Portnummer des Proxy-Servers ein. Der Proxy-Server muss Daten über Port 3101 an „<*Region*>.bbsecure.com“ senden können.

4. Klicken Sie auf **Speichern**.

Aktivieren von SOCKS v5 auf einem TCP-Proxy-Server

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

1. Klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Proxy**.
2. Wählen Sie die Option **Proxy-Server**.
3. Aktivieren Sie das Kontrollkästchen **SOCKS v5 aktivieren**.
4. Klicken Sie auf +.
5. Geben Sie in das Feld **Serveradresse** die IP-Adresse oder den Hostnamen des SOCKS v5-Proxy-Servers ein.
6. Klicken Sie auf **Hinzufügen**.
7. Wiederholen Sie die Schritte 1 bis 6 für jeden zu konfigurierenden SOCKS v5-Proxy-Server.
8. Geben Sie im Feld **Port** die Portnummer ein.
9. Klicken Sie auf **Speichern**.

Installieren eines eigenständigen BlackBerry Router

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.

Hinweis: Wenn Ihre aktuelle Umgebung einen TCP-Proxy-Server enthält, müssen Sie den BlackBerry Router nicht installieren.

Eigenständigen BlackBerry Router installieren

Bevor Sie beginnen:

- Sie müssen einen eigenständigen BlackBerry Router auf einem Computer installieren, der keine anderen BlackBerry UEM-Komponenten hostet. Sie können den BlackBerry Router nicht auf einem Computer installieren, der BlackBerry Connectivity Node hostet.
- Stellen Sie sicher, dass Sie den Namen des SRP-Hosts kennen. Der SRP-Hostname ist üblicherweise `<Ländercode>.srp.blackberry.com` (z. B. *de*`.srp.blackberry.com`). Um den SRP-Hostnamen Ihres Landes zu überprüfen, gehen Sie auf die Seite zur SRP-Adress-Suche.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > BlackBerry Cloud Connector**.
2. Klicken Sie auf **BlackBerry Connectivity Node hinzufügen**.
3. Klicken Sie im Abschnitt **Schritt 1: Herunterladen von BlackBerry Connectivity Node** auf **Herunterladen**.
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. Doppelklicken Sie auf die Datei **Setup.exe**.

   Die Installation läuft im Hintergrund und zeigt keine Dialogfelder an. Sobald die Installation abgeschlossen ist, erscheint im Fenster „Dienste“ der BlackBerry Router-Dienst.

Senden von Daten über den BlackBerry Router an die BlackBerry Infrastructure

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

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.

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

Konfigurieren von BlackBerry UEM für die Verwendung von BlackBerry Router

Bevor Sie beginnen: Eigenständigen BlackBerry Router installieren.

1. Klicken Sie in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) auf **Allgemeine Einstellungen > Proxy**.
2. Wählen Sie die Option **BlackBerry Router**.
3. Klicken Sie auf +.
4. Geben Sie die IP-Adresse oder den Hostnamen der BlackBerry Router-Instanz ein, zu der BlackBerry UEM eine Verbindung herstellen soll.
5. Klicken Sie auf **Hinzufügen**.
6. Wiederholen Sie die Schritte 1 bis 5 für jede BlackBerry Router-Instanz, die Sie konfigurieren möchten.
7. Geben Sie in das Feld **Port** die Portnummer ein, die von allen BlackBerry Router-Instanzen überwacht wird. Der Standardwert ist 3102.
8. Klicken Sie auf **Speichern**.

Verbinden von BlackBerry UEM mit Microsoft Azure

Microsoft Azure ist der Microsoft-Cloud-Computing-Service für die Bereitstellung und Verwaltung von Anwendungen und Services.

Das Verbinden von BlackBerry UEM mit Azure bietet Ihrem Unternehmen die folgenden Funktionen:

- Verbinden von BlackBerry UEM mit Azure Active Directory und Erstellen von Verzeichnisbenutzerkonten in BlackBerry UEM durch Suchen und Importieren von Benutzerdaten aus dem Unternehmensverzeichnis. 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.
- Verwenden von BlackBerry UEM zum Bereitstellen von iOS- und Android-Apps, die von Microsoft Intune verwaltet werden.
- Verwalten von Windows 10-Apps in BlackBerry UEM

Wenn Ihr Unternehmen Microsoft Active Directory anstatt von Azure Active Directory verwendet, um eine Verbindung mit Azure herzustellen, ist die Installation der neuesten Version von BlackBerry Connectivity Node erforderlich, damit BlackBerry UEM Cloud auf Ihr Firmenverzeichnis zugreifen kann.

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

Schritt	Aktion
1	Erstellen eines Microsoft Azure-Kontos.
2	Wenn Ihr Unternehmen Azure Active Directory verwendet, konfigurieren Sie BlackBerry UEM Cloud für die Synchronisierung mit Azure Active Directory.
3	Wenn Ihr Unternehmen ein lokales Microsoft Active Directory verwendet und Sie BlackBerry UEM verwenden möchten, um von Microsoft Intune verwaltete Apps bereitzustellen oder Windows 10-Apps zu verwalten, Synchronisieren von Microsoft Active Directory mit Microsoft Azure.
4	Erstellen Sie Unternehmensanwendungen in Azure, um zu ermöglichen, dass BlackBerry UEM Cloud eine Verbindung zu Microsoft Intune und Windows Store für Unternehmen herstellt.
5	Konfigurieren Sie BlackBerry UEM für die Synchronisierung mit Microsoft Intune und Windows Store für Unternehmen.

Erstellen eines Microsoft Azure-Kontos

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

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

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

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

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

Konfigurieren von BlackBerry UEM für die Synchronisierung mit Azure Active Directory

Wenn Ihr Unternehmen Microsoft Azure Active Directory verwendet, können Sie es mit BlackBerry UEM verbinden, um Verzeichnisbenutzerkonten in BlackBerry UEM zu erstellen, indem Sie nach Benutzerdaten im Unternehmensverzeichnis suchen und diese importieren. Verzeichnisbenutzer können ihre Verzeichnisanmeldeinformationen für den Zugriff auf BlackBerry UEM Self-Service verwenden.

Sie können eine Verbindung zu mehr als einer Instanz von Azure Active Directory herstellen. Nach der Installation von BlackBerry Connectivity Node ist auch eine Verbindung mit einem lokalen Verzeichnis möglich.

1. Melden Sie sich beim Azure-Portal an, und navigieren Sie zu der App, die Ihr Unternehmen verwendet, um Verbindungen zu Azure Active Directory zu ermöglichen

   Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration.
2. Fügen Sie Ihre BlackBerry UEM Cloud-Mandanten-URL zur Liste **URLs weiterleiten** für die App hinzu, und klicken Sie auf **Speichern**.
3. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
4. Klicken Sie auf + neben **Microsoft Azure Active Directory-Verbindung**.
5. Geben Sie einen **Namen der Verbindung des Verzeichnisses** und die **Domäne** für Ihr Azure Active Directory ein.
6. Klicken Sie auf **Fortfahren**.
7. Geben Sie die Microsoft-Benutzer-ID und das Kennwort für die App ein.
8. Klicken Sie auf **Annehmen**.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Verknüpfen von Unternehmensverzeichnisgruppen mit BlackBerry UEM-Gruppen

Synchronisieren von Microsoft Active Directory mit Microsoft Azure

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

Bevor Sie beginnen: Erstellen eines Microsoft Azure-Kontos

1. Laden Sie Azure AD Connect von http://www.microsoft.com/en-us/download/details.aspx?id=47594 herunter.
2. Installieren Sie die Azure AD Connect-Software.

3. Konfigurieren Sie Azure AD Connect für die Verbindung mit Ihrem firmeninternen Active Directory mit dem AzureActive Directory.

Wenn Sie fertig sind: Erstellen eines Unternehmensendpunkts in Azure

Erstellen eines Unternehmensendpunkts in Azure

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

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

Bevor Sie beginnen:

- Wenn Ihre Organisation ein lokales Microsoft Active Directory verwendet, Synchronisieren von Microsoft Active Directory mit Microsoft Azure
- Wenn Sie die moderne Authentifizierung verwenden, stellen Sie sicher, dass Sie über die Antwort-URL verfügen. Anweisungen zum Abrufen der Antwort-URL für die moderne Authentifizierung finden Sie unter Konfigurieren von BlackBerry UEM für die Synchronisierung mit Microsoft Intune.

1. melden Sie sich beim Azure-Portal an.
2. Navigieren Sie zu **Microsoft Azure > Azure Active Directory > App-Registrierungen**.
3. Klicken Sie auf **Endpunkte**.
4. Kopieren Sie den Wert unter **OAuth 2.0-Token-Endpunkt (v1)**, und fügen Sie ihn in eine Textdatei ein.

   Dies ist der **OAuth 2.0-Token-Endpunkt**, der in BlackBerry UEM erforderlich ist.
5. Schließen Sie die Liste **Endpunkte**, und klicken Sie auf **Neue Registrierung**.
6. Geben Sie im Feld **Name** einen Namen für die Anwendung ein.
7. Wählen Sie aus, welche Kontotypen die Anwendung verwenden oder auf die API zugreifen können.
8. Wählen Sie im Abschnitt **URI umleiten** in der Dropdown-Liste **Web** aus, und geben Sie eine gültige URL ein. Das URL-Format ist https://<*FQDN des BlackBerry UEM-Servers*>:<*port*>/admin/intuneauth
   - Wenn Sie die Authentifizierung über Client-Anmeldedaten verwenden oder nicht über eine registrierte Domäne verfügen, können Sie `http://localhost/` verwenden.
   - Wenn Sie eine moderne Authentifizierung verwenden, geben Sie die Antwort-URL aus BlackBerry UEM ein. Weitere Anweisungen finden Sie unter Konfigurieren von BlackBerry UEM für die Synchronisierung mit Microsoft Intune.
9. Klicken Sie auf **Registrieren**.
10. Kopieren Sie die **Anwendungs-ID** Ihrer Anwendung, und fügen Sie sie in eine Textdatei ein.

    Dies ist die **Client-ID**, die in BlackBerry UEM erforderlich ist.
11. Wenn Sie die Anwendung zur Verwendung von Microsoft Intune erstellen, klicken Sie auf **API-Berechtigungen** im Abschnitt **Verwalten**. Führen Sie folgende Schritte aus:
    a) Klicken Sie auf **Berechtigung hinzufügen**.
    b) Wählen Sie **Microsoft Graph**.
    c) Wählen Sie **Delegierte Berechtigungen** aus.
    d) Blättern Sie in der Liste der Berechtigungen nach unten, und legen Sie unter **Delegierte Berechtigungen** die folgenden Berechtigungen für Microsoft Intune fest:

- Microsoft Intune-Apps lesen und schreiben (**DeviceManagementApps > DeviceManagementApps.ReadWrite.All**)
- Alle Gruppen lesen (**Gruppe > Group.Read.All**)
- Basisprofil aller Benutzer lesen (**Benutzer > User.ReadBasic.All**)

e) Klicken Sie auf **Berechtigung hinzufügen**.
f) Klicken Sie unter **Einwilligung erteilen** auf **Administratoreinwilligung erteilen**.

Hinweis: Nur globale Administratoren können Berechtigungen gewähren.

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

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

12. Klicken Sie im Abschnitt **Verwalten** auf **Zertifikate und Schlüssel**. Führen Sie folgende Aktionen aus:

a) Klicken Sie unter **Client-Schlüssel** auf **Neuer Client-Schlüssel**.
b) Geben Sie eine Beschreibung für den Client-Schlüssel ein.
c) Wählen Sie eine Dauer für den Client-Schlüssel aus.
d) Klicken Sie auf **Hinzufügen**.
e) Kopieren Sie den Wert des neuen Client-Schlüssels.

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

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

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

Verknüpfen von Unternehmensverzeichnisgruppen mit BlackBerry UEM-Gruppen

Sie können Gruppen in BlackBerry UEM erstellen, die mit Gruppen in Ihrem Unternehmensverzeichnis verknüpft sind. Wenn Sie verzeichnisverknüpfte Gruppen aktivieren, können Sie folgende Funktionen nutzen:

- Hinzufügen von Gruppen in BlackBerry UEM, die mit Unternehmensverzeichnisgruppen verknüpft sind, zur Zuweisung und Verwaltung von IT-Richtlinien, Profilen und Apps für Benutzer. Diese Gruppen werden als verzeichnisverknüpfte Gruppen bezeichnet.

  Weitere Informationen zum Erstellen von verzeichnisverknüpften Gruppen finden Sie in der Dokumentation für Administratoren.
- Hinzufügen von Gruppen in BlackBerry UEM, die mit Unternehmensverzeichnisgruppen verknüpft sind, zur automatischen Synchronisierung der Gruppenmitgliedschaft. Diese Gruppen werden als Onboarding-Verzeichnisgruppen bezeichnet. Siehe Aktivieren von Onboarding.

Aktivieren von per Verzeichnis verknüpften Gruppen

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

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

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

   Die Standardeinstellung ist 5. Falls die Anzahl der zu synchronisierenden Änderungen das Synchronisierungslimit übersteigt, können Sie die Ausführung der Synchronisierung verhindern. Änderungen werden berechnet, indem die folgenden Elemente addiert werden: die den Gruppen hinzuzufügenden Benutzer, die aus den Gruppen zu entfernenden Benutzer, die per Onboarding zu integrierenden Benutzer, die durch Offboarding zu entfernenden Benutzer.
6. Geben Sie im Feld **Maximale Verschachtelung von Verzeichnisgruppen** die Anzahl der Verschachtelungsebenen ein, die für Unternehmensverzeichnisgruppen synchronisiert werden sollen.
7. Klicken Sie auf **Speichern**.

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

Aktivieren von Onboarding

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

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

Offboarding

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

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

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

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

Synchronisierung

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

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

Aktivieren und Konfigurieren von Onboarding und Offboarding

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

Bevor Sie beginnen:

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf den Namen des zu bearbeitenden Unternehmensverzeichnisses.

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

    Offboarding-Schutz bedeutet, dass Benutzer erst zwei Stunden nach dem nächsten Synchronisierungszyklus von BlackBerry UEM gelöscht werden.
11. Um die Synchronisierung von Unternehmensverzeichnisgruppen zu erzwingen, aktivieren Sie das Kontrollkästchen **Synchronisierung erzwingen**.

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

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

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

Synchronisieren einer Unternehmensverzeichnis-Verbindung

Bevor Sie beginnen: Vorschau des Synchronisationsberichts

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

Wenn Sie fertig sind: Anzeigen eines Synchronisierungsberichts

Vorschau des Synchronisationsberichts

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

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

Anzeigen eines Synchronisierungsberichts

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

Hinzufügen eines Synchronisationsplans

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

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

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Unternehmensverzeichnis**.
2. Klicken Sie auf den Namen des zu bearbeitenden Unternehmensverzeichnisses.
3. Klicken Sie auf der Registerkarte **Synchronisierungszeitplan** auf +.

4. Um die Menge der zu synchronisierenden Informationen zu reduzieren, wählen Sie in der Dropdown-Liste **Synchronisierungstyp** eine der folgenden Optionen aus:
   - **Alle Gruppen und Benutzer**: Dies ist die Standardeinstellung. Wenn Sie diese Option auswählen, erfolgt das Onboarding, Offboarding und die Verlinkung von Benutzern in per Verzeichnis verknüpften Gruppen während der Synchronisierung. Benutzer, die nicht integriert oder entfernt werden, aber die per Verzeichnis verknüpften Gruppen ändern, und Benutzer, deren Attribute geändert werden, werden synchronisiert.
   - **On-Boarding-Gruppen**: Wenn Sie diese Option auswählen, erfolgt das Onboarding, Offboarding und die Verlinkung von Benutzern in per Verzeichnis verknüpften Gruppen während der Synchronisierung. Benutzer, deren Attribute geändert werden, werden synchronisiert. Benutzer, die nicht integriert oder entfernt werden, aber die per Verzeichnis verknüpften Gruppen ändern, werden nicht synchronisiert.
   - **Per Verzeichnis verknüpfte Gruppen**: Wenn Sie diese Option auswählen, erfolgt das Onboarding und Offboarding von Benutzern nicht während der Synchronisierung. Benutzer, deren per Verzeichnis verknüpfte Gruppen geändert werden, werden entsprechend verknüpft. Benutzer, deren Attribute geändert werden, werden synchronisiert.
   - **Benutzerattribute**: Wenn Sie diese Option auswählen, erfolgt das Onboarding und Offboarding von Benutzern nicht während der Synchronisierung. Benutzer, deren per Verzeichnis verknüpfte Gruppen geändert werden, werden nicht synchronisiert. Benutzer, deren Attribute geändert werden, werden synchronisiert.
5. Wählen Sie in der Dropdown-Liste **Wiederholung** eine der folgenden Optionen aus:

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

6. Klicken Sie auf **Hinzufügen**.

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

APNs ist der Apple Push Notification Service. Sie müssen das APNs-Zertifikat abrufen und registrieren, wenn Sie BlackBerry UEM für die Verwaltung von iOS- oder macOS-Geräten verwenden möchten.

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

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

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

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

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

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

Abrufen einer signierten CSR-Datei von BlackBerry

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Wenn Sie noch kein APNs-Zertifikat haben, klicken Sie im Abschnitt **Schritt 1 von 3 - Signiertes CSR-Zertifikat von BlackBerry herunterladen** auf **Zertifikat herunterladen**.

   Wenn Sie ein aktuell verwendetes APNs-Zertifikat erneuern möchten, klicken Sie stattdessen auf **Zertifikat erneuern**.
3. Klicken Sie auf **Speichern**, um die signierte CSR-Datei (.scsr) auf Ihrem Computer zu speichern.

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

Anfordern eines APNs-Zertifikats von Apple

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie im Abschnitt **Schritt 2 von 3 – APNs-Zertifikat von Apple anfordern** auf **Apple Push Certificates Portal**. Sie werden zum Apple Push Certificates Portal weitergeleitet.
3. Melden Sie sich beim Apple Push Certificates Portal mit einer gültigen Apple-ID an.
4. Befolgen Sie die Anweisungen zum Hochladen der signierten CSR-Datei (.scsr).
5. Laden Sie das APNs-Zertifikat (.pem) auf Ihren Computer herunter, und speichern Sie es.
6. (Optional) Klicken Sie auf , um das Fenster **Hinweis** anzuzeigen.
7. Geben Sie im Fenster **Hinweis** die Apple-ID ein, die Sie zum Anfordern des APNs-Zertifikats verwendet haben. Sie müssen dieselbe Apple-ID verwenden, um das Zertifikat zu erneuern.
8. Klicken Sie auf eine beliebige Stelle außerhalb des Fensters **Hinweis**, um es zu schließen.

Wenn Sie fertig sind: Registrieren des APNs-Zertifikats.

Registrieren des APNs-Zertifikats

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

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

Wenn Sie fertig sind: Zum Testen der Verbindung zwischen BlackBerry UEM und dem APNs-Server klicken Sie auf **APNs-Zertifikat testen**.

Erneuern des APNs-Zertifikats

Das APNs-Zertifikat ist ein Jahr lang gültig. Sie müssen das APNs-Zertifikat jährlich vor dem Ablaufdatum erneuern. Das Zertifikat muss mit derselben Apple-ID erneuert werden, die Sie zum Abrufen des ursprünglichen APNs-Zertifikats verwendet haben.

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

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie auf **Zertifikat erneuern**.
3. Klicken Sie im Abschnitt **Schritt 1 von 3 – Signiertes CSR-Zertifikat von BlackBerry herunterladen** auf **Zertifikat herunterladen**.
4. Klicken Sie auf **Speichern**, um die signierte CSR-Datei (.scsr) auf Ihrem Computer zu speichern.
5. Klicken Sie im Abschnitt **Schritt 2 von 3 – APNs-Zertifikat von Apple anfordern** auf **Apple Push Certificates Portal**. Sie werden zum Apple Push Certificates Portal weitergeleitet.
6. Melden Sie sich beim Apple Push Certificates Portal mit derselben Apple-ID an, die Sie zum Abrufen des ursprünglichen APNs-Zertifikats verwendet haben.

7. Befolgen Sie die Anweisungen zum Erneuern des APNs-Zertifikats (.pem). Sie müssen die neue signierte CSR hochladen.
8. Laden Sie das erneuerte APNs-Zertifikat auf Ihren Computer herunter, und speichern Sie es.
9. Klicken Sie im Abschnitt **Schritt 3 von 3 – APNs-Zertifikat registrieren** auf **Durchsuchen**. Navigieren Sie zu dem erneuerten APNs-Zertifikat, und wählen Sie es aus.
10. Klicken Sie auf **Senden**.

Wenn Sie fertig sind: Zum Testen der Verbindung zwischen BlackBerry UEM und dem APNs-Server klicken Sie auf **APNs-Zertifikat testen**.

Fehlerbehebung: APNs

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

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

Beschreibung

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

Mögliche Lösung

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

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

Beschreibung

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

Mögliche Lösung

Gehen Sie auf https://support.blackberry.com/community/s/article/37266, und lesen Sie Artikel 37266.

Ich kann iOS- oder macOS-Geräte nicht aktivieren

Problemursache

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

Mögliche Lösung

Führen Sie eine oder mehrere der folgenden Aktionen aus:

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

Konfigurieren von BlackBerry UEM für DEP

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

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

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

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

Erstellen eines DEP-Kontos

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie in **Schritt 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.

Wenn Sie fertig sind: Herunterladen eines öffentlichen Schlüssels.

Herunterladen eines öffentlichen Schlüssels

Bevor Sie beginnen: Erstellen eines DEP-Kontos.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple-Programm zur Geräteregistrierung**.
2. Klicken Sie auf +.

3. Klicken Sie in Schritt **2 von 4: Herunterladen eines öffentlichen Schlüssels** auf **Herunterladen des öffentlichen Schlüssels**.
4. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Generieren eines Server-Tokens.

Generieren eines Server-Tokens

Bevor Sie beginnen: Herunterladen eines öffentlichen Schlüssels.

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

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

Registrieren des Server-Tokens bei BlackBerry UEM

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

Bevor Sie beginnen: Generieren eines Server-Tokens.

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

Wenn Sie fertig sind: Hinzufügen der ersten Registrierungskonfiguration.

Hinzufügen der ersten Registrierungskonfiguration

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

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

1. Geben Sie einen Namen für die Konfiguration ein.
2. Führen Sie eine der folgenden Aufgaben aus:

- Wenn Sie möchten, dass BlackBerry UEM Geräten bei der Registrierung im Apple-Programm zur Geräteregistrierung automatisch die Registrierungskonfiguration zuweist, aktivieren Sie das Kontrollkästchen „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“.
- Wenn Sie die BlackBerry UEM-Konsole verwenden möchten, um die Registrierungskonfiguration manuell bestimmten Geräten zuzuweisen, deaktivieren Sie das Kontrollkästchen „Alle neuen Geräte automatisch dieser Konfiguration zuweisen“.

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

6. Klicken Sie auf **Speichern**.

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

Wenn Sie fertig sind: Aktivieren Sie iOS-Geräte. Weitere Informationen zum Aktivieren von beim DEP registrierten Geräten finden Sie in der Dokumentation für Administratoren.

Aktualisieren des Server-Tokens

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

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

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

Entfernen einer DEP-Verbindung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Entfernen der Verbindung zu Ihrer Google-Domäne

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

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

- Deaktivieren einer BlackBerry UEM-Domäne
- Verbinden einer anderen BlackBerry UEM-Instanz mit der Google Cloud- oder G Suite-Domäne

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration**.
2. Klicken Sie auf **Google-Domänenverbindung**.
3. Klicken Sie auf **Verbindung entfernen**.

4. Klicken Sie auf **Entfernen**.

Entfernen der Google-Domänenverbindung mithilfe Ihres Google-Kontos

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

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

Bearbeiten oder Testen der Google-Domänenverbindung

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

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

Vereinfachung von Windows 10-Aktivierungen

Sie können BlackBerry UEM in Azure Active Directory integrieren, um den Registrierungsprozess für Windows 10-Geräte zu vereinfachen. Nach der Konfiguration können Benutzer ihre Geräte mit UEM unter Zuhilfenahme ihres Azure Active Directory-Benutzernamens und -Kennworts registrieren.

Integration von UEM mit Azure Active Directory Join

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

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

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

UEM mit Azure Active Directory integrieren

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

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

Konfiguration von Windows Autopilot in Microsoft Azure

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

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

Erstellen eines Windows Autopilot-Bereitstellungsprofils in Azure

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

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

Importieren von Windows Autopilot-Geräten nach Azure

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

1. Schalten Sie das Windows 10-Gerät ein, um das Gerät sofort einzurichten.
2. Stellen Sie eine Verbindung zu einem Wi-Fi-Netzwerk mit Internetverbindung her.
3. Drücken Sie auf der Tastatur **STRG + UMSCHALT + F3** oder **STRG+Fn+UMSCHALT+F3**. Das Gerät wird neu gestartet und wechselt in den Überwachungsmodus.
4. Führen Sie **Windows PowerShell** als Administrator aus.
5. Führen Sie `Save-Script -Name Get-WindowsAutoPilotInfo -Pfad C:\Windows\Temp` aus, um das Windows PowerShell-Skript zu überprüfen.
6. Führen Sie `Install Script -Name Get-WindowsAutoPilotInfo` aus, um das Skript zu installieren.
7. Führen Sie `Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv` aus, um die Geräteinformationen in einer .csv-Datei zu speichern.
8. Gehen Sie folgendermaßen vor, um eine .csv-Datei in Microsoft Azure zu importieren:
   a) Navigieren Sie im Azure-Portal zu **Geräteregistrierung > Windows-Registrierung > Windows AutoPilot-Geräte**.
   b) Klicken Sie auf **Importieren**.
   c) Wählen Sie die .csv-Datei aus.
9. Führen Sie im Dialogfeld **Systemvorbereitungstool** die folgenden Schritte aus:
   a) Wählen Sie im Feld **Systembereinigungsaktion** die Option **Out-of-Box-Experience (OOBE) für System aktivieren** aus, und deaktivieren Sie die Option **Verallgemeinern**.
   b) Wählen Sie im Feld **Optionen für Herunterfahren** die Option **Neustart** aus.

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

Befolgen Sie die Anweisungen in diesem Abschnitt zur Konfiguration von BlackBerry UEM Cloud zur Unterstützung von BlackBerry Dynamics-Apps.

Verwalten von BlackBerry Proxy-Clustern

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

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

Aufgabe	Schritte
Erstellen Sie ein neues BlackBerry Proxy-Cluster.	**a.** Klicken Sie auf +. **b.** Geben Sie einen Namen für das Cluster ein. **c.** Klicken Sie auf **Speichern**.
Benennen Sie ein BlackBerry Proxy-Cluster um.	**a.** Klicken Sie auf einen Clusternamen. **b.** Ändern Sie den Namen des Clusters. Jedes Cluster muss über einen eindeutigen Namen verfügen. **c.** Klicken Sie auf **Speichern**.
Verschieben Sie eine BlackBerry Proxy-Instanz in ein anderes BlackBerry Proxy-Cluster.	**a.** Klicken Sie in der Spalte **Server** auf den Namen einer BlackBerry Proxy-Instanz. **b.** Wählen Sie in der Dropdown-Liste BlackBerry Proxy**Cluster** das Cluster aus, zu dem die Instanz hinzugefügt werden soll. **c.** Klicken Sie auf **Speichern**.
Löschen Sie ein leeres BlackBerry Proxy-Cluster.	**a.** Klicken Sie auf × für dieses Cluster. **b.** Klicken Sie auf **Entfernen**.
App-Proxyeinstellungen für ein Cluster festlegen	**a.** Klicken Sie auf **Einstellungen > BlackBerry Dynamics > Cluster**. **b.** Klicken Sie auf den Clusternamen. **c.** Klicken Sie auf **Globale Einstellungen überschreiben**. Weitere Informationen finden Sie unter Konfigurieren von Proxyeinstellungen für die BlackBerry Dynamics-App für den BlackBerry Cloud Connector.

Aufgabe	Schritte
PAC-Dateiaktualisierungen für alle Cluster herunterladen	• Klicken Sie auf **PAC-Cache aktualisieren**.
Vertrauenswürdiges Stammzertifikat angeben, 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.** Wählen Sie das zu verwendende E-Mail-Profil aus. **f.** Klicken Sie auf **Öffnen**. **g.** Geben Sie eine Beschreibung für das Zertifikat ein. **h.** Klicken Sie auf **Hinzufügen**.

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**.
2. Klicken Sie auf **Direct Connect**.
3. Klicken Sie auf eine BlackBerry Proxy-Instanz.
4. Um Direct Connect zu aktivieren, markieren Sie das Kontrollkästchen **Direct Connect aktivieren**. Überprüfen Sie im Feld **BlackBerry Proxy-Hostname** den Hostnamen auf Richtigkeit. Wenn der von Ihnen erstellte öffentliche DNS-Eintrag vom FQDN des Servers abweicht, geben Sie stattdessen den externen FQDN an.
5. Wiederholen Sie die Schritte 3 und 4 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 BlackBerry Proxy-Cluster verwalten in der Dokumentation zur Konfiguration.
6. Klicken Sie auf **Speichern**.

Verbindung von BlackBerry Proxy mit BlackBerry Dynamics NOC

Wenn Sie BlackBerry Proxy verwenden möchten, damit BlackBerry Dynamics-Apps eine Verbindung zu den Ressourcen Ihres Unternehmens herstellen können, muss die Firewall Ihres Unternehmens TCP-Verbindungen für

die folgenden IP-Bereiche zulassen, sodass BlackBerry Proxy eine Verbindung mit dem BlackBerry Dynamics NOC herstellen kann:

- 206.124.114.1 bis 206.124.114.254 (206.124.114.0/24) auf Port 443
- 206.124.121.1 bis 206.124.121.254 (206.124.121.0/24) auf Port 443
- 206.124.122.1 bis 206.124.122.254 (206.124.122.0/24) auf Port 443

Alternativ besteht die Möglichkeit, die Firewall Ihres Unternehmens so zu konfigurieren, dass Verbindungen zu den folgenden Hostnamen unterstützt werden:

- gdentgw.good.com auf Port 443
- gdrelay.good.com auf Port 443
- gdweb.good.com auf Port 443
- gdmdc.good.com auf Port 443

Überschreiben globaler HTTP-Proxyeinstellungen für einen BlackBerry Connectivity Node

Wenn BlackBerry Connectivity Node installiert ist, können Sie globale BlackBerry UEM Cloud-Proxyeinstellungen überschreiben, um BlackBerry Dynamics-App-Daten über einen HTTP-Proxy zwischen BlackBerry Proxy und einem Anwendungsserver zu senden. 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 BlackBerry UEM-Proxyeinstellungen. Weitere Informationen finden Sie im Administrationshandbuch für BlackBerry Access.

Hinweise zu PAC-Dateien

Wenn Sie PAC-Dateien mit BlackBerry Proxy verwenden, sollten Sie die folgenden Support-Hinweise beachten.

BlackBerry UEM unterstützt die folgenden PAC-Datei-Richtlinien:

- DIRECT
- PROXY (als HTTPS-Proxy behandelt - Verbindung wird über HTTP CONNECT hergestellt)
- HTTPS (Verbindung wird über HTTP CONNECT hergestellt)

BlackBerry UEM unterstützt die folgenden PAC-Datei-Richtlinien nicht:

- BLOCK (als DIRECT behandelt)
- SOCKS (Verbindungsfehler)
- SOCKS4 (Verbindungsfehler)
- SOCKS5 (Verbindungsfehler)
- HTTP (Verbindungsfehler)
- Benutzerdefinierte NATIVE-Anweisung, die von BlackBerry Access definiert wird (Verbindungsfehler)

Für BlackBerry UEM gelten die folgenden zusätzlichen Einschränkungen für PAC-Dateien:

- 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.

Konfigurieren von Proxyeinstellungen für die BlackBerry Dynamics-App für BlackBerry Cloud Connector

Sie können BlackBerry Cloud Connector-Proxyeinstellungen für BlackBerry Dynamics-Apps manuell oder mithilfe einer PAC-Datei konfigurieren.

1. Klicken Sie in BlackBerry Cloud Connector auf **Allgemeine Einstellungen > BlackBerry Router und Proxy**.
2. Wählen Sie **Globale Einstellungen** aus.
3. Wählen Sie eine der folgenden Optionen aus:
   - **HTTP-Proxy manuell aktivieren**
   - **PAC aktivieren**

   PAC-Dateien werden nur für Verbindungen zu Anwendungsservern unterstützt. Wenn Sie beide Optionen konfigurieren, hat die PAC-Konfiguration Vorrang für Verbindungen zu Anwendungsservern. PAC-Dateien werden nur für Apps unterstützt, die mit BlackBerry Dynamics SDK 7.0 und höher entwickelt wurden.
4. Wenn Sie **HTTP-Proxy manuell aktivieren** ausgewählt haben, führen Sie die folgenden Schritte aus:
   a) Wählen Sie eine der folgenden Optionen aus.
      - **Über Proxy nur mit NOC-Servern von BlackBerry Dynamics verbinden**
      - **Über Proxy mit allen Servern verbinden**
      - **Über Proxy nur mit bestimmten Servern verbinden**

   b) Wenn Sie den Proxy verwenden möchten, um eine Verbindung mit den angegebenen Servern herzustellen, klicken Sie auf +, um zusätzliche Server anzugeben.
   c) Geben Sie in das Feld **Adresse** die Adresse für den Proxyserver ein.
   d) Geben Sie im Feld **Port** die vom Proxyserver überwachte Portnummer ein.
   e) Wenn die in der PAC-Datei angegebenen Proxyserver eine Authentifizierung benötigen, wählen Sie **Authentifizierung verwenden**, und legen Sie den **Benutzernamen**, das **Kennwort** und bei Bedarf die **Domäne** fest, die die App für die Authentifizierung verwenden soll.
5. Wenn Sie **PAC aktivieren** ausgewählt haben, führen Sie die folgenden Schritte aus:
   a) Geben Sie im Feld **PAC-URL** die URL für die PAC-Datei ein.
   b) Wenn der Proxy-Server eine Authentifizierung benötigt, wählen Sie **Authentifizierung verwenden**, und legen Sie den **Benutzernamen**, das **Kennwort** und bei Bedarf die **Domäne** fest, die die App für die Authentifizierung verwenden soll.

      Zugangsdaten für die Endbenutzerauthentifizierung werden für die Proxyauthentifizierung nicht unterstützt.
6. Klicken Sie auf **Speichern**.

Konfigurieren von E-Mail-Benachrichtigungen für BlackBerry Work

BEMS Cloud nimmt Push-Registrierungsanfragen von Geräten an, wie z. B. iOS und Android, und kommuniziert dann mit dem lokalen Microsoft Exchange Server- oder Microsoft Office 365-Server, um das Postfach des Benutzers auf Änderungen hin zu überprüfen. Wenn Sie die Informationen über den lokalen Microsoft Exchange Server oder den Microsoft Office 365-Server angeben, nennen Sie die Einstellungen für die Erstellung des BEMS-Cloudmandanten für Ihr Unternehmen.

Wenn der Mandant erstellt wird, werden die folgenden Dienste automatisch aktiviert:

- BlackBerry Directory Lookup: Dieser Service ermöglicht es Benutzern, weitere Benutzer nach Vorname, Nachname und zugehörigem Foto oder Avatar im Firmenverzeichnis zu suchen.
- BlackBerry Follow-Me: Diese Funktion unterstützt BlackBerry Dynamics Launcher auf BlackBerry Work.

Bevor Sie beginnen:

- Prüfen Sie, dass auf dem Dienstkonto Berechtigungen für die Impersonation einer Anwendung angewandt wurden.
- Wenn Sie die moderne Authentifizierung aktivieren möchten, stellen Sie sicher, dass Sie in einer Microsoft Office 365-Umgebung die folgenden Schritte ausgeführt haben:
  - Wenn Sie die moderne Authentifizierung mithilfe der Authentifizierung der Anmeldeinformationen aktiviert haben, rufen Sie die Client-Anwendungs-ID ab.
  - Wenn Sie die moderne Authentifizierung mithilfe der Client-Zertifikat-Authentifizierung aktivieren, befolgen Sie einen dieser Schritte:
    - Rufen Sie die Client-Anwendungs-ID mit zertifikatbasierter Authentifizierung auf
    - Erstellen und verknüpfen Sie ein selbst signiertes .pfx-Zertifikat zur Azure-App-ID für BEMS

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > E-Mail-Benachrichtigungen**.
2. Wählen Sie im Abschnitt **Authentifizierungstyp** einen Authentifizierungstyp basierend auf Ihrer Umgebung und führen Sie die damit verbundenen Aufgaben durch, sodass BEMS mit Microsoft Exchange Server oder Microsoft Office 365 kommunizieren kann:

Authentifizierungst	Beschreibung	Aufgabe
Anmeldeinformationen	Diese Option verwendet den BEMS-Benutzernamen und das Kennwort, um sich bei Microsoft Exchange Server oder Microsoft Office 365 zu authentifizieren.	**a.** Geben Sie im Feld **Benutzername des Dienstkontos** den Benutzernamen für das BEMS-Dienstkontos ein. • Geben Sie für Microsoft Office 365 den Benutzerprinzipalnamen (User Principal Name, UPN) des Dienstkontos ein. • Verwenden Sie für lokale Microsoft Exchange Server das Format <*Domäne*>\<*Benutzername*>. **b.** Geben Sie im Feld **Kennwort des Dienstkontos** das Kennwort für das Dienstkonto ein.
Client-Zertifikat	Diese Option verwendet ein Client-Zertifikat, damit sich das BEMS-Dienstkonto bei Microsoft Exchange Server oder Microsoft Office 365 authentifizieren kann.	**a.** Klicken Sie neben dem Feld **Zertifikatsdatei (.pfx),** auf **Durchsuchen**. Navigieren Sie zu der Client-Zertifikatsdatei und wählen Sie sie aus. **b.** Geben Sie im Feld **Kennwort** das Kennwort für das Client-Zertifikat ein.

3. Wenn Sie eine Verbindung zu einer Microsoft Office 365-Umgebung herstellen, führen Sie die folgenden Schritte aus, um die moderne Authentifizierung zu aktivieren:
   a) Aktivieren Sie das Kontrollkästchen **Moderne Authentifizierung aktivieren**.
   b) Geben Sie im Feld **Authentifizierungsstelle** die Authentifizierungsserver-URL ein, auf die BEMS zugreift, um die OAuth-Token zur Authentifizierung mit Microsoft Office 365 (z. B. https://login.microsoftonline.com/<*Mandantenname*>) abzurufen.
   c) Geben Sie im Feld **Client-Anwendungs-ID** eine der folgenden Azure-App-IDs ein, je nach Authentifizierungstyp, den Sie ausgewählt haben. Führen Sie einen der folgenden Schritte aus, um die Azure-App-ID zu erhalten:
      - #unique_82
      - Abrufen einer Azure-App-ID für BEMS mit zertifikatbasierter Authentifizierung
   d) Geben Sie in das Feld **Servername** den FQDN des Microsoft Office 365-Servers ein.

e) Wählen Sie optional das Kontrollkästchen **Anmeldeinformationen verwenden, wenn die moderne Authentifizierung fehlgeschlagen ist**, um BEMS die Kommunikation mit Microsoft Office 365 zu ermöglichen, falls BEMS nicht auf die moderne Authentifizierungsquelle zugreifen kann. Wenn Sie dieses Kontrollkästchen wählen, müssen Sie die Anmeldeinformationen für das BEMS-Dienstkonto bereitstellen.

Hinweis: Wenn Sie die moderne Authentifizierung konfigurieren, verwenden alle Knoten die angegebene Konfiguration.

4. Geben Sie im Feld **Benutzername des Dienstkontos** den Benutzernamen ein, der zum Anmelden beim Microsoft Exchange Server- oder Microsoft Office 365-Server verwendet wird. Der Benutzername muss in einem der folgenden Formate eingegeben werden:
   - Wenn in Ihrer Umgebung ein lokaler Microsoft Exchange Server verwendet wird, nutzen Sie <*Domäne*>\<*Benutzername*> oder UPN.
   - Wenn in Ihrer Umgebung Microsoft Office 365 verwendet wird, nutzen Sie <*Benutzername*>@<*Domäne*>.com.
5. Geben Sie im Feld **Kennwort des Dienstkontos** das Kennwort für den Benutzernamen des Dienstkontos ein, den Sie bereitgestellt haben.
6. Optional können Sie im Feld **Autodiscover-URL** die URL für Autodiscover eingeben, damit BEMS Benutzerinformationen über Microsoft Exchange Server oder den Microsoft Office 365-Server abrufen kann, wenn Benutzer für BlackBerry Push Notifications erkannt werden.

   Hinweis: Wenn Sie keine URL eingeben, verwendet BEMS Autodiscover zum Suchen von Microsoft Exchange Server oder dem Microsoft Office 365-Server, um Informationen zum Benutzer abzurufen.
7. Wählen Sie das Kontrollkästchen **HTTP-Umleitung und DNS SRV-Datensatz zulassen** aus, um HTTP-Umleitung und DNS SRV-Abfragen für das Abrufen der Autodiscover-URL bei der Ermittlung von Benutzern für BlackBerry Push Notifications zuzulassen. Standardmäßig ist diese Funktion aktiviert.
8. Wählen Sie **BlackBerry Connectivity Node-Verbindung aktivieren**, um BEMS Cloud zu erlauben, eine Verbindung mit der BlackBerry Infrastructure herzustellen, statt einen eingehenden Port zu verwenden. Diese Einstellung erfordert, dass BlackBerry Connectivity Node installiert und in Ihrer Umgebung konfiguriert ist.
9. Optional können Sie im Feld **E-Mail-Adresse des Benutzers** eine E-Mail-Adresse zum Testen der Verbindung zu Microsoft Exchange Server oder zum Microsoft Office 365-Server eingeben.
10. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Testen Sie die Verbindung zum lokalen Microsoft Exchange Server oder zum Microsoft Office 365-Server und zu Autodiscover. Aktualisieren Sie den Bildschirm „E-Mail-Benachrichtigungen“, oder öffnen Sie ihn erneut. Klicken Sie auf **Testen**.
  Hinweis: Stellen Sie sicher, dass der Verbindungstest erfolgreich war, bevor Sie Geräte bereitstellen, um Probleme mit der automatischen Erkennung zu vermeiden. Wenn die Geräte vor der Konfiguration des E-Mail-Benachrichtigungsdienstes aktiviert werden, müssen sich Benutzer bei BlackBerry Work abmelden und dann erneut einloggen.
- Weisen Sie die Black Cloud Enterprise-Dienste (com.blackberry.gdservice-entitlement.cloud) Benutzern zu, um E-Mail-Benachrichtigungen für BlackBerry Work zu erhalten. Weitere Informationen finden Sie in der folgenden BlackBerry UEM Cloud-Dokumentation für Administratoren:
  - Zuweisen einer App zu einem Benutzer
  - Zuweisen einer App-Gruppe zu einer Benutzergruppe
  - Zuweisen einer App zu einem Benutzerkonto
  - Zuweisen einer App oder App-Gruppe zu einem Benutzerkonto
- Erstellen Sie optional eine vertrauenswürdige Verbindung zwischen der BEMS Cloud und Microsoft Exchange Server. Anweisungen finden Sie unter Herstellen einer vertrauenswürdigen Verbindung zwischen BEMS Cloud und Microsoft Exchange Server.

- Konfigurieren Sie BlackBerry Work. Weitere Anweisungen finden Sie in der Dokumentation zu BlackBerry Work, Notes und Tasks für Administratoren.

Gewähren von Berechtigungen für den Anwendungsidentitätswechsel für das -Dienstkonto

Damit der BlackBerry Push Notifications-Dienst Postfächer auf Updates überwacht, braucht das BlackBerry Push Notifications-Dienstkonto Berechtigungen für den Identitätswechsel.

Führen Sie den folgenden Microsoft Exchange Management Shell-Befehl aus, um Berechtigungen für den Anwendungsidentitätswechsel auf das -Dienstkonto anzuwenden:

1. Öffnen Sie Microsoft Exchange Management Shell.
2. Geben Sie `New-ManagementRoleAssignment -Name:<ImpersonationAssignmentName> -Role:ApplicationImpersonation -User:<ServiceAccount>` ein. Zum Beispiel `New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User:BlackBerryAdmin`.

Wenn Sie fertig sind:

Weitere Informationen zum Beschränken der Berechtigungen für den Anwendungsidentitätswechsel für bestimmte Benutzer, Unternehmenseinheiten oder Sicherheitsgruppen finden Sie in der MSDN-Bibliothek unter Vorgehensweise: Konfigurieren eines Identitätswechsels.

Gewähren von Berechtigungen für den Anwendungsidentitätswechsel mit Exchange Administration Center

1. Melden Sie sich je nach Umgebung bei einer der folgenden Konsolen an:

Konsole	Schritte
Microsoft Office 365 Exchange Administration Center-Konsole	**a.** Melden Sie sich bei https://portal.office.com an. **b.** Klicken Sie auf das App-Startfeld-Symbol in der oberen linken Ecke. **c.** Klicken Sie auf **Administrator**. **d.** Klicken Sie im **Microsoft 365 Admin Center**-Konsolenmenü auf **Alle anzeigen**. **e.** Klicken Sie im Abschnitt **Admin Center** auf **Alle Admin Center**. **f.** Klicken Sie auf **Exchange**.
Webkonsole des lokalen Microsoft Exchange Administration Centers	**a.** Öffnen Sie einen Browser unter `https://<url_to_on-premises_client_access_server>/ecp`, und melden Sie sich mit einem gültigen Konto an.

2. Klicken Sie auf **Berechtigungen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für die Rollengruppe ein.
5. Klicken Sie im Abschnitt **Rollen** auf +. Klicken Sie auf **ApplicationImpersonation > Hinzufügen > OK**.
6. Klicken Sie im Abschnitt **Mitglieder** auf +. Klicken Sie auf ein Konto, das Sie hinzufügen möchten, und klicken Sie dann auf **Hinzufügen > OK**.

Abrufen einer Azure-App-ID für BEMS mit zertifikatbasierter Authentifizierung

1. Melden Sie sich bei „portal.azure.com“ an.
2. Klicken Sie in der linken Spalte auf **Azure Active Directory**.
3. Klicken Sie auf **App registrations**.

4. Klicken Sie auf **New application registration**.
5. Geben Sie im Feld **Name** einen Namen für die Anwendung ein.
6. Wählen Sie in der Dropdown-Liste **Anwendungstyp** die Option **Web-App/API** aus.
7. Geben Sie im Feld **Anmelde-URI** `http://<In Schritt 5 erteilter Name der App>` ein.
   Diese App ist ein Daemon, keine Web-App, und hat keine Anmelde-URL.
8. Drücken Sie die **Eingabetaste**.
9. Klicken Sie auf **Erstellen**.
10. Wählen Sie den Namen der Anwendung, die Sie erstellt haben.
11. Klicken Sie auf **Einstellungen**.
12. Klicken Sie in der Spalte **Einstellungen** auf **Eigenschaften**.
13. Kopieren Sie in der Spalte **Eigenschaften** die **Apple-ID-URI**.
14. Klicken Sie auf **Required permissions**.
15. Klicken Sie auf **Hinzufügen**.
16. Klicken Sie auf .
17. Wählen Sie **Office 365 Exchange Online (Microsoft Exchange)Select an API**.
18. Klicken Sie auf **Select**.
19. Wählen Sie im Abschnitt **App-Berechtigungen auswählen** das Kontrollkästchen **Exchange Web Service mit vollem Zugriff auf alle Postfächer verwenden**.
20. Klicken Sie auf **Select**.
21. Klicken Sie auf **Fertig**.
22. Klicken Sie auf **Berechtigungen gewähren**.
23. Klicken Sie auf **Ja**.
24. Klicken Sie auf **Hinzufügen**.
25. Klicken Sie auf **Eine API auswählen**
26. Klicken Sie auf **Microsoft Graph**.
27. Klicken Sie auf **Select**.
28. Wählen Sie im Abschnitt **Delegierte Berechtigungen** das Kontrollkästchen **Anmelden und Benutzerprofil lesen**.
29. Klicken Sie auf **Select**.
30. Klicken Sie auf **Fertig**.
31. Klicken Sie auf **Berechtigungen gewähren**.
32. Klicken Sie auf **Ja**.
33. Kopieren Sie die **Anwendungs-ID**. Die Anwendungs-ID wird auf der Hauptseite **App-Registrierungen** für die angegebene App angezeigt. Sie wird als **Client-Anwendungs-ID** verwendet.
34. Schließen Sie „portal.azure.com“ nicht.

Wenn Sie fertig sind: Verknüpfen eines Zertifikats mit der Azure-App-ID für BEMS

Verknüpfen eines Zertifikats mit der Azure-App-ID für BEMS

Sie können ein vorhandenes Zertifikat von Ihrem Server der Zertifizierungsstelle oder dem Befehl „Neues selbst signiertes Zertifikat“ verwenden, um ein selbst signiertes Zertifikat zu erstellen. Weitere Informationen finden Sie unter docs.microsoft.com im Abschnitt „Neues selbst signiertes Zertifikat“.

Bevor Sie beginnen: Vergewissern Sie sich, dass Sie den App-Namen, den Sie in BEMS mit zertifikatbasierter Authentifizierung zugewiesen haben, kennen.

1. Wenn Sie ein vom Server der Zertifizierungsstelle ausgestelltes Zertifikat haben, fahren Sie mit Schritt 2 fort. Erstellen Sie ein selbst signiertes Zertifikat.

a) Öffnen Sie auf dem Computer, auf dem Microsoft Windows ausgeführt wird, die Windows PowerShell.
b) Geben Sie den folgenden Befehl ein: `$cert=New-SelfSignedCertificate -Subject "CN=<App-Name>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`.
   - Wobei <*App-Name*> der Name ist, den Sie der App in Schritt 5 unter Abrufen einer Azure-App-ID für BEMS mit zertifikatbasierter Authentifizierung zugewiesen haben.
c) Drücken Sie die **Eingabetaste**.

2. Exportieren Sie das Zertifikat aus dem Zertifikat-Manager. Dadurch wird ein öffentliches Zertifikat erstellt. Stellen Sie sicher, dass Sie das öffentliche Zertifikat als .CER oder .PEM speichern.
   a) Öffnen Sie auf dem Computer, auf dem Windows ausgeführt wird, den Zertifikat-Manager für den angemeldeten Benutzer.
   b) Erweitern Sie **Personal**.
   c) Klicken Sie auf **Zertifikate**.
   d) Klicken Sie mit der rechten Maustaste auf <*Benutzer*>@<*Domäne*> und klicken Sie auf **Alle Aufgaben > Exportieren**.
   e) Klicken Sie im **Assistent zum Exportieren für Zertifikate** auf **Nein, privaten Schlüssel nicht exportieren**.
   f) Klicken Sie auf **Weiter**.
   g) Wählen Sie **Base-64 encoded X.509 (.CER)**. Klicken Sie auf **Weiter**.
   h) Geben Sie einen Namen für das Zertifikat ein und speichern Sie es auf Ihrem Desktop.
   i) Klicken Sie auf **Weiter**.
   j) Klicken Sie auf **Fertigstellen**.
   k) Klicken Sie auf **OK**.
3. Laden Sie das öffentliche Zertifikat hoch, um die Anmeldeinformationen des Zertifikats mit der Azure-App-ID für BEMS zu verknüpfen.
   a) Öffnen Sie im portal.azure.com den <*App-Namen*>, den Sie der App in Schritt 5 unter Abrufen einer Azure-App-ID für BEMS mit zertifikatbasierter Authentifizierung zugewiesen haben.
   b) Klicken Sie auf **Einstellungen > Schlüssel**.
   c) Klicken Sie auf **Öffentlichen Schlüssel hochladen**.
   d) Klicken Sie auf und navigieren Sie zu dem Speicherort, an dem Sie das Zertifikat in Schritt 2 exportiert haben.
   e) Klicken Sie auf **Öffnen**.
   f) Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Exportieren Sie das Zertifikat im .pfx-Format mit dem MMC Snap-In zur Verwaltung von Benutzerzertifikaten. Stellen Sie sicher, dass Sie den privaten Schlüssel mit aufnehmen. Anweisungen finden Sie unter docs.microsoft.com im Abschnitt „Exportieren eines Zertifikats mit dem privaten Schlüssel“.

Herstellen einer vertrauenswürdigen Verbindung zwischen BEMS Cloud und Microsoft Exchange Server

Wenn Sie E-Mail-Benachrichtigungen für BlackBerry Work aktivieren und der Microsoft Exchange Server Ihres Unternehmens kein SSL-Zertifikat verwendet, das von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde, ist die Verbindung zwischen BEMS Cloud und Microsoft Exchange Server nicht vertrauenswürdig. Zum Herstellen einer vertrauenswürdigen Verbindung zum Microsoft Exchange Server laden Sie das SSL-Zertifikat des Servers (oder die Stamm- oder Zwischenzertifizierungskette) in die BEMS Cloud-Datenbank hoch. Die .pem-Datei kann ein oder mehrere SSL-Zertifikate enthalten.

Bevor Sie beginnen:

- Konfigurieren Sie die E-Mail-Benachrichtigungen für BlackBerry Work. Anweisungen finden Sie unter Konfigurieren von E-Mail-Benachrichtigungen für BlackBerry Work.

- Exportieren Sie das SSL-Zertifikat vom Microsoft Exchange Server im verschlüsselten .pem base64-Format, und speichern Sie es an einem Netzwerkspeicherort, auf den Sie über die Verwaltungskonsole zugreifen können.
- Wenn Sie mehr als ein SSL-Zertifikat hochladen, müssen diese sich in einer einzelnen .pem-Datei befinden. Durch das Hochladen von mehr als einer Datei werden alle vorhandenen SSL-Zertifikate in der BEMS-Datenbank ersetzt.

1. Klicken Sie in der Menüleiste auf **Einstellungen > BlackBerry Dynamics**.
2. Klicken Sie auf **E-Mail-Benachrichtigungen**.
3. Klicken Sie auf die Registerkarte **Zertifikate**.
4. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Speicherort der .pem-Datei, die Sie hochladen möchten.
5. Klicken Sie auf **Speichern**.

Ersetzen oder Löschen der SSL-Zertifikate für vertrauenswürdige Verbindungen

Wenn Sie die SSL-Zertifikate ersetzen (z. B. wenn die Zertifikate ablaufen), ersetzen Sie alle vorhandenen SSL-Zertifikate in der BEMS-Datenbank. Wenn Sie mehr als ein SSL-Zertifikat in die .pem-Datei aufgenommen haben, überprüfen Sie, ob alle Zertifikate wie erforderlich im neuen Upload enthalten sind.

Hinweis: Wenn Sie die SSL-Zertifikate löschen, entfernen Sie alle SSL-Zertifikate in der Datenbank und die vertrauenswürdige Verbindung.

Bevor Sie beginnen:

- Exportieren Sie die neuen SSL-Zertifikate vom Microsoft Exchange Server im verschlüsselten .pem base64-Format, und speichern Sie sie an einem Netzwerkspeicherort, auf den Sie über die Verwaltungskonsole zugreifen können. Weitere Informationen zu digitalen Zertifikaten und zur Verschlüsselung im Microsoft Exchange Server finden Sie unter https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016
- Wenn Sie mehrere SSL-Zertifikate hochladen, müssen diese sich in einer einzelnen .pem-Datei befinden.

1. Klicken Sie in der Menüleiste auf **Einstellungen > BlackBerry Dynamics**.
2. Klicken Sie auf **E-Mail-Benachrichtigungen**.
3. Klicken Sie auf die Registerkarte **Zertifikate**.
4. Klicken Sie auf .
5. Klicken Sie auf **Ersetzen**.
6. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Speicherort des Zertifikats, das Sie hochladen möchten.
7. Klicken Sie auf **Speichern**.

Konfigurieren von BEMS-Docs

Mithilfe der BlackBerry UEM-Konsole können Sie Dokument- und Datei-Repositorys und Benutzerzugriffsrichtlinien für mobile App-Benutzer des Dienstes konfigurieren und verwalten. Wenn dieser Dienst aktiviert ist, können Benutzer über die folgenden Speicherdienste auf Dokumente zugreifen, diese synchronisieren und freigeben: Microsoft SharePoint Online, Microsoft SharePoint, Microsoft OneDrive for Business und Box. Anbieter von Dateifreigabe- und CMIS-basierten Repository-Speichern werden nicht unterstützt.

Hinweis: Wenn Ihre Umgebung den Zugriff von Benutzern auf Dateifreigaben oder CMIS-basierte Repositorys erfordert, konfigurieren Sie BEMS-Docs in einer lokalen BEMS-Instanz. Die Aktivierung von BEMS-Docs in BlackBerry UEM Cloud und in einer lokalen BEMS-Instanz in einer BlackBerry UEM Cloud-Umgebung wird nicht unterstützt. Weitere Informationen finden Sie unter Konfigurieren eines lokalen BEMS in einer BlackBerry UEM Cloud-Umgebung.

Repositorys: Der BEMS-Docs-Dienst bietet Ihren Benutzern Zugriff auf gespeicherte geschäftliche Daten von ihren mobilen Geräten aus. Auf einem geschäftlichen Server ist ein Docs-Repository (auch „Freigabe“ genannt) vorhanden. Das Repository enthält Dateien, die von autorisierten Benutzern freigegeben wurden. Weitere Informationen zum Einrichten und Verwalten Ihrer Freigaben in BlackBerry UEM und des zugehörigen Benutzerzugriffs finden Sie unter Verwalten von Repositorys. Bevor Sie Ihre Repositorys konfigurieren, aktivieren und konfigurieren Sie den BEMS-Docs-Dienst und konfigurieren Sie BlackBerry Work in BlackBerry UEM, damit Ihre Benutzer vom ihrem Gerät auf die Repositorys zugreifen können, die Sie hinzufügen und definieren.

Speicherdienste: Der BEMS-Docs-Dienst unterstützt eine Reihe von Speicherdiensten.

Aktivieren des BEMS-Docs-Dienstes

Damit Benutzer in Ihrer Umgebung auf Dokument- und Datei-Repositorys zugreifen können, müssen Sie den BEMS-Docs-Dienst aktivieren. Wenn Sie diesen Dienst aktivieren, wird ein BEMS-Mandant erstellt, und dem BlackBerry Dynamics-Verbindungsprofil wird die Berechtigung für den BlackBerry Cloud Docs-Dienst (com.blackberry.gdservice-permission.docs.cloud) hinzugefügt. Wenn Ihre Umgebung sowohl den BEMS-Docs-Dienst als auch die E-Mail-Benachrichtigungen für BlackBerry Work verwendet, konfigurieren Sie zuerst die E-Mail-Benachrichtigungen. Anweisungen finden Sie unter Konfigurieren von E-Mail-Benachrichtigungen für BlackBerry Work.

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf **Aktivieren**.

BEMS-Docs-Einstellungen konfigurieren

Bevor Sie beginnen:

- Überprüfen Sie, ob der BEMS-Docs-Dienst aktiviert ist.
- Wenn Ihre Umgebung für Microsoft SharePoint Online oder Azure-IP konfiguriert ist, stellen Sie sicher, dass die BlackBerry Work-App in Azure registriert ist, damit sie auf die BEMS-Docs Azure-App zugreifen kann. Weitere Anweisungen finden Sie unter Abrufen einer Azure-App-ID für BlackBerry Work in der Dokumentation zu BlackBerry Work, Notes und Tasks für Administratoren.
- Wenn Ihre Umgebung für Azure-IP konfiguriert ist, halten Sie die folgenden Informationen bereit:
  - Azure-Mandantenname
  - Azure-Anwendungs-ID für den BEMS-Dienst
  - Azure-Anwendungsschlüssel für den BEMS-Dienst
- Wenn BEMS-Docs für die Kommunikation mit einer lokalen Microsoft SharePoint-Instanz konfiguriert ist, stellen Sie sicher, dass Microsoft SharePoint-Repositorys sichere HTTPS-Ports verwenden. Die Verwendung von nicht sicheren HTTP-Ports wird nicht unterstützt.

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf die Registerkarte **Einstellungen**.
3. Führen Sie eine oder beide der folgenden Aufgaben aus.

Umgebung	Schritte
Ihre Umgebung ist für die Verwendung von Microsoft SharePoint Online oder Azure-IP und Microsoft SharePoint Online konfiguriert	**a.** Aktivieren Sie optional das Kontrollkästchen **Azure-Informationsschutz aktivieren**, um BEMS-Docs die Authentifizierung bei Azure-IP zu ermöglichen. **b.** Geben Sie den Azure-Mandantennamen ein. **c.** Geben Sie die Azure-Anwendungs-ID für den BEMS-Dienst ein, die Sie bei der Registrierung des BEMS-Docs-Komponentendienstes erhalten haben. Weitere Anweisungen finden Sie unter Abrufen einer Azure-App-ID für den BEMS-Docs-Komponentendienst. **d.** Geben Sie den Azure-Anwendungsschlüssel für den BEMS-Dienst ein, die Sie bei der Registrierung der Docs-App in Azure erhalten haben. Weitere Anweisungen finden Sie unter Abrufen einer Azure-App-ID für den BEMS-Docs-Komponentendienst.
Ihre Umgebung ist für die Verwendung einer lokalen Microsoft SharePoint-Instanz konfiguriert	**a.** Aktivieren Sie das Kontrollkästchen **BlackBerry Connectivity Node-Verbindung aktivieren**, um BEMS zu erlauben, eine Verbindung mit der BlackBerry Infrastructure herzustellen, statt einen eingehenden Port zu verwenden. Diese Einstellung erfordert, dass BlackBerry Connectivity Node installiert und in Ihrer Umgebung konfiguriert ist. **b.** Um BEMS-Docs die Kommunikation mit einem lokalen Microsoft SharePoint-Server zu ermöglichen, extrahieren Sie das Microsoft SharePoint-Serverzertifikat und senden es an den BlackBerry-Support. Wenn die lokalen Microsoft SharePoint-Sites Zertifikate verwenden, die nicht öffentlich vertrauenswürdig sind (z. B. selbstsignierte oder Unternehmens-CA-Zertifikate), senden Sie diese Zertifikate an den BlackBerry-Support.

4. Klicken Sie auf **Speichern**.

Abrufen einer Azure-App-ID für den BEMS-Docs-Komponentendienst

Wenn Ihre Umgebung für Microsoft SharePoint Online, Microsoft OneDrive for Business oder Microsoft Azure-IP konfiguriert ist, müssen Sie die BEMS-Komponentendienste in Azure registrieren.

Wenn Ihre Umgebung sowohl Microsoft SharePoint Online und Microsoft Azure-IP oder Microsoft OneDrive for Business und Microsoft Azure-IP verwendet, müssen Sie den Microsoft SharePoint Online- oder Microsoft OneDrive for Business-Dienst registrieren. Microsoft Azure-IP verwendet die gleichen Informationen wie der registrierte Dienst.

Bevor Sie beginnen: Um Berechtigungen zu erteilen, müssen Sie ein Konto mit Mandantenadministratorberechtigungen verwenden.

1. Melden Sie sich bei portal.azure.com an.
2. Klicken Sie in der linken Spalte auf **Azure Active Directory**.
3. Klicken Sie auf **App-Registrierungen**.
4. Klicken Sie auf **Neue Registrierung**.
5. Geben Sie im Feld **Name** einen Namen für die Anwendung ein. Beispiel: AzureAppIDfuerBEMS.
6. Wählen Sie einen unterstützten Kontotyp aus.
7. Wählen Sie in der Dropdown-Liste **Umleitungs-URI** die Option **Web** aus, und geben Sie `https://localhost:8443` ein.
8. Klicken Sie auf **Registrieren**.
9. Notieren Sie sich die **Anwendungs-(Client)-ID**. Dieser Wert wird als **Azure-App-ID für BEMS-Dienst** in der BlackBerry UEM-Verwaltungskonsole verwendet.

10. Klicken Sie im Abschnitt **Verwalten** auf **API-Berechtigungen**.
11. Klicken Sie auf **Berechtigung hinzufügen**.
12. Klicken Sie im Abschnitt **API auswählen** auf **APIs, die mein Unternehmen verwendet**.
13. Wenn Ihre Umgebung für Azure-IP konfiguriert ist, suchen Sie nach **Microsoft Information Protection Sync Service**, und klicken Sie darauf. Legen Sie die folgende Berechtigung fest:
    - Aktivieren Sie in den delegierten Berechtigungen das Kontrollkästchen **Alle einheitlichen Richtlinien lesen, auf die ein Benutzer Zugriff hat** (**UnifiedPolicy > UnifiedPolicy.User.Read**).
14. Klicken Sie auf **Berechtigung hinzufügen**.
15. Klicken Sie auf **Berechtigung hinzufügen**.
16. Führen Sie eine oder mehrere der folgenden Aufgaben aus:

Dienst	Berechtigungen
Zur Konfiguration von Docs für die Verwendung von Microsoft SharePoint Online oder Microsoft OneDrive for Business	**a.** Klicken Sie auf **SharePoint**. **b.** Legen Sie die folgenden Berechtigungen fest: • Deaktivieren Sie in den Anwendungsberechtigungen alle Berechtigungen. **1.** Klicken Sie auf **Anwendungsberechtigungen**. **2.** Klicken Sie auf **Alle erweitern**. Stellen Sie sicher, dass alle Optionen deaktiviert sind. • Aktivieren Sie in den delegierten Berechtigungen das Kontrollkästchen **Lese- und Schreibzugriff auf Elemente und Listen in allen Sitesammlungen** (**AllSite > AllSites.Manage**). **c.** Klicken Sie auf **Berechtigung hinzufügen**.
Wenn Sie Microsoft Azure-IP verwenden	**a.** Klicken Sie auf **Microsoft Graph**. Wenn Microsoft Graph nicht aufgeführt ist, fügen Sie Microsoft Graph hinzu. **b.** Legen Sie die folgenden Berechtigungen fest: • Aktivieren Sie in den Anwendungsberechtigungen das Kontrollkästchen **Lesezugriff auf Verzeichnisdaten** (**Directory > Directory.Read.All**). • Aktivieren Sie in den delegierten Berechtigungen das Kontrollkästchen **Lesezugriff auf Verzeichnisdaten** (**Directory > Directory.Read.All**). **c.** Klicken Sie auf **Berechtigungen aktualisieren**.

17. Klicken Sie auf **Administratoreinwilligung gewähren**. Klicken Sie auf **Ja**.

    Wichtig: Für diesen Schritt sind Mandantenadministratorrechte erforderlich.
18. Damit die automatische Erkennung wie erwartet funktioniert, legen Sie die Authentifizierungsberechtigungen fest. Führen Sie die folgenden Schritte aus:
    a) Klicken Sie im Abschnitt **Verwalten** auf **Authentifizierung**.
    b) Aktivieren Sie im Abschnitt **Implizite Genehmigung** das Kontrollkästchen **ID-Token**.
    c) Wählen Sie im Feld **Standard-Clienttyp** die Option **Nein** aus.
    d) Klicken Sie auf **Speichern**.
19. Definieren Sie den Geltungsbereich und die Vertrauensstellung für diese API. Klicken Sie im Abschnitt **Verwalten** auf **Eine API verfügbar machen**. Führen Sie folgende Aufgaben durch.

Aufgabe	Schritte
Hinzufügen eines Bereichs	Der Bereich schränkt den Zugriff auf Daten und Funktionen ein, die durch die API geschützt werden. **a.** Klicken Sie auf **Bereich hinzufügen**. **b.** Klicken Sie auf **Speichern und fortfahren**. **c.** Füllen Sie die folgenden Felder aus und nehmen Sie die folgenden Einstellungen vor: • Bereichsname: Geben Sie einen eindeutigen Namen für den Bereich an. • Wer kann zustimmen: Klicken Sie auf **Administratoren und Benutzer**. • Anzeigename der Administratoreinwilligung: Geben Sie einen beschreibenden Namen ein. • Beschreibung der Administratoreinwilligung: Geben Sie eine Beschreibung für den Bereich ein. • Status: Klicken Sie auf **Aktiviert**. Standardmäßig ist der Status „Aktiviert“. **d.** Klicken Sie auf **Bereich hinzufügen**.
Hinzufügen einer Client-Anwendung	Die Autorisierung einer Client-Anwendung bedeutet, dass die API der Anwendung vertraut und Benutzer nicht zur Zustimmung aufgefordert werden sollten. **a.** Klicken Sie auf **Eine Client-Anwendung hinzufügen**. **b.** Geben Sie im Feld **Client-ID** die Client-ID ein, die Sie in Schritt 9 oben aufgezeichnet haben. **c.** Aktivieren Sie das Kontrollkästchen **Autorisierte Bereiche**, um den Tokentyp anzugeben, der vom Dienst zurückgegeben wird. **d.** Klicken Sie auf **Anwendung hinzufügen**.

20. Klicken Sie im Bereich **Verwalten** auf **Zertifikate und geheime Schlüssel**, und fügen Sie einen geheimen Client-Schlüssel hinzu. Führen Sie die folgenden Schritte aus:

a) Klicken Sie auf **Neuer geheimer Client-Schlüssel**.
b) Geben Sie im Feld **Beschreibung** eine Beschreibung für den Schlüssel mit maximal 16 Zeichen einschließlich Leerzeichen ein.
c) Legen Sie ein Ablaufdatum fest (z. B. „In 1 Jahr“, „In 2 Jahren“, „Läuft nie ab“).
d) Klicken Sie auf **Hinzufügen**.
e) Kopieren Sie den **Wert** des Schlüssels.

Wichtig: Der Wert ist nur verfügbar, wenn Sie ihn erstellen. Sie können nicht mehr darauf zugreifen, nachdem Sie die Seite verlassen haben. Dieser Wert wird als **Azure-Anwendungsschlüssel für BEMS-Dienst** in der BlackBerry UEM-Konsole verwendet.

Zulassen der Authentifizierung für BEMS-Docs mit einer alternativen E-Mail-Adresse

Sie können die BEMS Cloud so konfigurieren, dass Benutzer sich bei Microsoft SharePoint Online und Microsoft OneDrive for Business mit einer E-Mail-Adresse authentifizieren können, die sich von der E-Mail-Adresse unterscheidet, die zur Installation und Aktivierung von BlackBerry Work verwendet wurde. Wenden Sie sich an den technischen Support von BlackBerry, um diese Funktion zu aktivieren.

Verwalten von Repositorys

BEMS Cloud verfügt über die folgenden Repository-Speicheranbieter:

Speicher-Repository	Beschreibung
SharePoint SharePoint Online	Ein sicherer Webserver mit freigegebenen Dateien, auf die über das Internet zugegriffen wird. Wenn Ihre Umgebung für Microsoft OneDrive for Business konfiguriert ist, wird das SharePoint Online-Speicher-Repository verwendet.
Box	Ein sicheres Cloud-Speicherkonto von box.com mit freigegebenen Dateien, auf die über das Internet zugegriffen werden kann.

Ein Repository wird im BEMS-Docs-Dienst weiter nach dem hinzufügenden und definierenden Benutzer kategorisiert.

Speicher-Repository	Beschreibung
Admin-definiert	Speicheranbieter-Websites, die von BlackBerry UEM-Administratoren hinzugefügt und verwaltet werden und auf die einzelnen Benutzern und Benutzergruppen Zugriff gewährt wird.
Benutzerdefiniert	Websites, die von einzelnen Endbenutzern von ihren mobilen Geräten hinzugefügt wurden. Sie als BlackBerry UEM-Administrator können den Zugriff über mobile Geräte auf diese Sites gemäß den Richtlinien für die zulässige Nutzung der IT-Abteilung Ihres Unternehmens deaktivieren und wieder aktivieren.

Konfigurieren von Repositorys

Die Repository-Konfigurationsseite verfügt über die folgenden beiden Registerkarten, die Sie konfigurieren können:

Registerkarten	Beschreibung
Admin-definiert	Ermöglicht das Erstellen und Verwalten von Repositorys, das Hinzufügen und Entfernen von Benutzern und Benutzergruppen sowie das Zuweisen von Dateizugriffs- und Dateinutzungsberechtigungen zu Benutzern und Benutzergruppen.
Benutzerdefiniert	Ermöglicht das Hinzufügen und Entfernen von Benutzern und Benutzergruppen, das Aktivieren und Deaktivieren der Möglichkeit zum Erstellen benutzerdefinierter Repositorys durch Benutzer und Benutzergruppen sowie das Erteilen und Widerrufen von Berechtigungen zum Ausführen einer Reihe von dateibezogenen Aktionen in den benutzerdefinierten Repositorys.

Admin-definierte Freigaben

Freigaben sind Dokument-Repositorys für einen bestimmten Speicheranbieter.

Wenn Sie Repositorys und Listen definieren, führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Definieren von Repositorys.
2	Definieren Sie Zugriffsberechtigungen für Benutzer und Benutzergruppen.

Erteilen von Benutzerzugriffsberechtigungen

Zugriffsberechtigungen werden für ein einzelnes Repository definiert oder von einer vorhandenen Repository-Liste übernommen. Berechtigungen können selektiv vorhandenen Microsoft Active Directory-Domänenbenutzern und -Benutzergruppen gewährt werden. Mindestens ein Benutzer oder eine Benutzergruppe muss der Repository-Definition hinzugefügt werden, um Zugriffsberechtigungen zu konfigurieren.

In der folgenden Tabelle sind die verfügbaren Zugriffsberechtigungen und Standardeinstellungen aufgeführt.

Berechtigung	Berechtigungsattribute	Standardeinstellung
Auflisten (Durchsuchen)	Anzeigen und Durchsuchen von Repository-Inhalten (z. B. Unterordner und Dateien) in einer angezeigten Liste und Sortieren von Listen nach Name, Datum, Größe oder Art	Aktiviert
Dateien löschen	Entfernen von Dateien aus dem Repository	Aktiviert
Lesen (Herunterladen)	Herunterladen von Repository-Dateien auf das Gerät des Benutzers und Öffnen zum Lesen	Aktiviert
Schreiben (Hochladen)	Hochladen von Dateien (neu/geändert) vom Gerät des Benutzers in das Repository zum dortigen Speichern	Aktiviert
Zwischenspeichern (Offlinedateien)	Vorübergehendes Speichern eines Caches von Repository-Dateien auf dem Gerät für den Offlinezugriff	Aktiviert
Öffnen mit	Öffnen einer Datei mit einer formatkompatiblen Anwendung auf dem Gerät	Aktiviert
Ordner erstellen	Hinzufügen neuer Ordner zum Repository	Aktiviert
Kopieren/ Einfügen	Kopieren des Inhalts der Repository-Datei und Einfügen in eine andere Datei oder Anwendung	Aktiviert
Einchecken/ Auschecken	Wenn eine Datei ausgecheckt ist, kann der Benutzer sie bearbeiten, schließen, erneut öffnen und offline mit der Datei arbeiten. Andere Benutzer können die Datei erst ändern und Änderungen erst sehen, wenn sie wieder eingecheckt wurde.	Aktiviert (nur SharePoint)
Freigabe-Link erstellen	Benutzer können einen Link zu einer Datei und einem Ordner erstellen und den Link an Empfänger senden. Für „Freigabe-Link erstellen“ ist eine aktualisierte BlackBerry Work-App erforderlich.	Aktiviert (nur Box)

Ändern von Zugriffsberechtigungen

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf **Repositorys**.
3. Klicken Sie auf die Registerkarte **Admin-definiert**.
4. Klicken Sie auf ein Repository.
5. Aktivieren oder deaktivieren Sie unter **Zugriffsberechtigungen** neben dem Benutzer oder der Benutzergruppe das Kontrollkästchen für die Berechtigung, die Sie ändern möchten.
6. Klicken Sie neben Benutzern oder Benutzergruppen, die Sie entfernen möchten, auf ⊗.
7. Klicken Sie auf **Speichern**.

Definieren von Repositorys

Microsoft Active Directory-Benutzer und -Gruppen müssen einer Repository-Definition hinzugefügt werden, bevor Zugriffsberechtigungen konfiguriert werden können. Hinzugefügte Benutzer und Gruppen erhalten automatisch die Standardzugriffsberechtigungen.

Bevor Sie beginnen: Damit Benutzer auf ihren Geräten auf ihre Microsoft SharePoint-Repositorys zugreifen können, müssen Sie sicherstellen, dass ihnen die Berechtigungsstufe „Lesen“ und die Berechtigung „Verzeichnisse durchsuchen“ zugewiesen sind.

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf **Repositorys**.
3. Klicken Sie auf die Registerkarte **Admin-definiert**.
4. Klicken Sie auf +.
5. Geben Sie unter im Feld **Name** den Namen des Repositorys ein, der Benutzern mit mobilem Zugriff auf das Repository angezeigt wird.

   Der Repository-Name muss eindeutig sein und darf Leerzeichen enthalten. Die folgenden Sonderzeichen können aufgrund von Beschränkungen Dritter nicht verwendet werden:

   - Microsoft SharePoint 2010, 2013 und 2016: ~ " # % & * : < > ? / \ { | }
   - Box: \ /|
6. Wählen Sie in der Dropdown-Liste **Speicher** einen Speicheranbieter aus.

   Wenn Sie **SharePoint** oder **SharePoint Online** auswählen und auf der Freigabe SharePoint 2013 oder höher ausgeführt wird, aktivieren Sie das Kontrollkästchen **Sites hinzufügen, denen Benutzer dieser Site folgen**, um diese Funktion für Benutzer dieser Freigabe verfügbar zu machen. Diese Einstellung gilt nur für persönliche (eigene) SharePoint- oder OneDrive for Business-Sites.

   Wenn Ihre Umgebung für Microsoft OneDrive for Business konfiguriert ist, wählen Sie den Speicheranbieter SharePoint Online aus.
7. Geben Sie im Feld **Pfad** den Pfad zur Freigabe an. Führen Sie je nach Speichertyp, den Sie in Schritt 6 ausgewählt haben, eine der folgenden Aufgaben aus.

Speichertyp	Beschreibung
Box	Geben Sie eine vollständig qualifizierte URL mit oder ohne Microsoft Active Directory-Attribute ein.

Speichertyp	Beschreibung
SharePoint SharePoint Online	Wenn Ihr Speicheranbieter Microsoft OneDrive for Business ist, führen Sie diese Aufgabe aus. Geben Sie eine vollständig qualifizierte URL mit oder ohne Microsoft Active Directory -Attribute ein. Um eigene („my“) oder persönliche SharePoint-Sites hinzuzufügen, geben Sie die URL für die persönliche Site an. Beispiel: • Wenn Ihre Umgebung SharePoint und SharePoint Online verwendet, https://<*Microsoft SharePoint-Server*>/my. • Wenn Ihre Umgebung Microsoft OneDrive for Business verwendet, *https://<Ihre O365-Domäne>-my.sharepoint.com/personal/admin_<domain>_onmicrosoft_com/_layouts/15/onedrive.aspx* Wenn die persönliche Site Benutzernamen oder andere Microsoft Active Directory-Attribute enthält, geben Sie den Pfad einschließlich dieser Attribute ein. Beispiel: https://<*Microsoft SharePoint-Server*>/my/<*SAMKontoname*>. Führen Sie optional die folgenden Schritte aus, um automatisch Sites hinzuzufügen, denen gefolgt wird: **a.** Fügen Sie ein Repository für die eigene („my“) oder persönliche SharePoint-Site hinzu. **b.** Wählen Sie **Sites hinzufügen, denen Benutzer dieser Site folgen** für das Repository aus. **c.** Aktivieren Sie auf der Registerkarte **Benutzerdefiniert** eine benutzerdefinierte Repository-Berechtigung. Stellen Sie sicher, dass Sie die Kontrollkästchen **Benutzerdefinierte Freigaben aktivieren** und **Sites, denen Benutzer folgen, automatisch hinzufügen** aktivieren. Anweisungen finden Sie unter Aktivieren benutzerdefinierter Repository-Berechtigungen.

8. Klicken Sie im Abschnitt **Zugriffsberechtigungen** auf +.
9. Wählen Sie eines der folgenden Elemente aus:
   - **Benutzer**: Geben Sie im Feld **Benutzer hinzufügen** eine vollständige oder teilweise Suchzeichenfolge ein. Klicken Sie auf den Benutzer, den Sie hinzufügen möchten.
   - **Gruppen**: Wählen Sie auf dem Bildschirm **Gruppe hinzufügen** eine oder mehrere Gruppen aus. Klicken Sie auf →. Klicken Sie auf **Hinzufügen**.
10. Klicken Sie auf **Hinzufügen**.
11. Klicken Sie auf **Speichern**.

Hinzufügen von Benutzern und Benutzergruppen zu Repositorys

Microsoft Active Directory-Benutzer und -Gruppen müssen einer Repository-Definition hinzugefügt werden, bevor Zugriffsberechtigungen konfiguriert werden können. Hinzugefügte Benutzer und Gruppen erhalten automatisch die Standardzugriffsberechtigungen.

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf **Repositorys**.
3. Klicken Sie auf die Registerkarte **Admin-definiert**.
4. Klicken Sie auf ein Repository.

5. Klicken Sie unter **Zugriffsberechtigungen** auf +.
6. Wählen Sie eines der folgenden Elemente aus:
   - **Benutzer**: Geben Sie im Feld **Benutzer hinzufügen** eine vollständige oder teilweise Suchzeichenfolge ein. Klicken Sie auf den Benutzer, den Sie hinzufügen möchten.
   - **Gruppen**: Wählen Sie auf dem Bildschirm **Gruppe hinzufügen** eine oder mehrere Gruppen aus. Klicken Sie auf →. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Erteilen Sie Benutzern und Benutzergruppen Zugriffsberechtigungen.

Bearbeiten von Repositorys

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf **Repositorys**.
3. Klicken Sie auf die Registerkarte **Admin-definiert**.
4. Klicken Sie auf ein Repository, das Sie bearbeiten möchten.
5. Nehmen Sie die erforderlichen Änderungen vor.
6. Klicken Sie auf **Speichern**.

Zulassen benutzerdefinierter Repositorys

Sie können Benutzern erlauben, eigene „benannte“ Datenquellen in Admin-definierten Repositorys zu definieren, für die sie bereits Berechtigungen erhalten haben.

Wenn Sie Benutzern erlauben, eigene Repositorys zu definieren, führen Sie die folgenden Aktionen aus:

1. Aktivieren benutzerdefinierter Repository-Berechtigungen
2. Ändern von Benutzerzugriffsberechtigungen

Aktivieren benutzerdefinierter Repository-Berechtigungen

Bevor Sie beginnen: Damit Benutzer auf ihren Geräten auf ihre Microsoft SharePoint-Repositorys zugreifen können, müssen Sie sicherstellen, dass ihnen die Berechtigungsstufe „Lesen“ und die Berechtigung „Verzeichnisse durchsuchen“ zugewiesen sind.

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf **Repositorys**.
3. Klicken Sie auf die Registerkarte **Benutzerdefiniert**.
4. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Freigaben aktivieren**, damit Ihre mobilen Benutzer ihre eigenen Datenquellen definieren können.
5. Aktivieren Sie optional das Kontrollkästchen **Sites, denen Benutzer folgen, automatisch hinzufügen** für autorisierte Microsoft SharePoint-Repositorys, für die das erforderliche MySite-Plug-In aktiviert ist.

   Führen Sie die folgenden Schritte aus, um automatisch Sites hinzuzufügen, denen gefolgt wird:

   a. Fügen Sie auf der Registerkarte „Admin-definiert“ ein Repository für die eigene („my“) oder persönliche SharePoint-Site hinzu. Anweisungen finden Sie unter Definieren von Repositorys.
   b. Wählen Sie **Sites hinzufügen, denen Benutzer dieser Site folgen** für das Repository aus.
   c. Stellen Sie auf der Registerkarte „Benutzerdefiniert“ sicher, dass Sie die Kontrollkästchen **Benutzerdefinierte Freigaben aktivieren** und **Sites, denen Benutzer folgen, automatisch hinzufügen** aktivieren.

6. Wählen Sie im Abschnitt **Speicher** einen oder mehrere Speicherdienste aus.

   Sie müssen mindestens eine Speicheroption auswählen, damit die benutzerdefinierte Option aktiviert werden kann.
7. Klicken Sie im Abschnitt **Zugriffsberechtigungen** auf +.
8. Wählen Sie **Benutzer** oder **Gruppen** aus.
9. Geben Sie im Feld **Benutzer hinzufügen** eine vollständige oder teilweise Suchzeichenfolge ein. Klicken Sie auf den Benutzer, den Sie hinzufügen möchten.
10. Wählen Sie auf dem Bildschirm **Gruppe hinzufügen** eine oder mehrere Gruppen aus. Klicken Sie auf →. Klicken Sie auf **Hinzufügen**.
11. Klicken Sie auf **Hinzufügen**. Die hinzugefügten Benutzer und Gruppen erhalten automatisch die Standardzugriffsberechtigungen.
12. Klicken Sie auf **Speichern**.

Zugriffsberechtigungen

Berechtigungen können selektiv vorhandenen Microsoft Exchange ActiveSync-Domänenbenutzern und -Benutzergruppen gewährt werden. Die restriktivsten Berechtigungen (vom Administrator oder vom Benutzer definiert) werden angewendet.

In der folgenden Tabelle sind die Berechtigungen aufgeführt, die standardmäßig bereitgestellt werden, wenn Sie Benutzer und Gruppen zu den benutzerdefinierten Repositorys hinzufügen.

Berechtigung	Berechtigungsattribute	Standardeinstellung
Auflisten (Durchsuchen)	Anzeigen und Durchsuchen von Repository-Inhalten (z. B. Unterordner und Dateien) in einer angezeigten Liste und Sortieren von Listen nach Name, Datum, Größe oder Art	Aktiviert
Dateien löschen	Entfernen von Dateien aus dem Repository	Aktiviert
Lesen (Herunterladen)	Herunterladen von Repository-Dateien auf das Gerät des Benutzers und Öffnen zum Lesen	Aktiviert
Schreiben (Hochladen)	Hochladen von Dateien (neu/geändert) vom Gerät des Benutzers in das Repository zum dortigen Speichern	Aktiviert
Zwischenspeichern (Offlinedateien)	Vorübergehendes Speichern eines Caches von Repository-Dateien auf dem Gerät für den Offlinezugriff	Aktiviert
Öffnen mit	Öffnen einer Datei mit einer formatkompatiblen Anwendung auf dem Gerät	Aktiviert
Ordner erstellen	Hinzufügen neuer Ordner zum Repository	Aktiviert
Kopieren/Einfügen	Kopieren des Inhalts der Repository-Datei und Einfügen in eine andere Datei oder Anwendung	Aktiviert

Berechtigung	Berechtigungsattribute	Standardeinstellung
Einchecken/Auschecken	Wenn eine Datei ausgecheckt ist, kann der Benutzer sie bearbeiten, schließen, erneut öffnen und offline mit der Datei arbeiten. Andere Benutzer können die Datei erst ändern und Änderungen erst sehen, wenn sie wieder eingecheckt wurde.	Aktiviert (nur SharePoint)
Neue Repositorys hinzufügen	Ermöglicht das Hinzufügen neuer Repositorys vom mobilen Gerät des Benutzers.	Deaktiviert
Freigabe-Link erstellen	Benutzer können einen Link zu einer Datei und einem Ordner erstellen und den Link an Empfänger senden. Für „Freigabe-Link erstellen“ ist eine aktualisierte BlackBerry Work-App erforderlich.	Aktiviert (nur Box)

Ändern von Benutzerzugriffsberechtigungen

1. Klicken Sie in der Verwaltungskonsole auf **Einstellungen > BlackBerry Dynamics > Docs**.
2. Klicken Sie auf **Repositorys**.
3. Klicken Sie auf die Registerkarte **Benutzerdefiniert**.
4. Aktivieren oder deaktivieren Sie unter **Zugriffsberechtigungen** neben dem Benutzer oder der Benutzergruppe das Kontrollkästchen für die Berechtigung, die Sie ändern möchten.
5. Klicken Sie neben Benutzern oder Benutzergruppen, die Sie entfernen möchten, auf ⊗.
6. Klicken Sie auf **Speichern**.

Konfigurieren eines lokalen BEMS in einer BlackBerry UEM Cloud-Umgebung

Sie können ein lokales BEMS so konfigurieren, dass es mit dem BlackBerry Proxy kommuniziert, um GDAuth-Token in einer BlackBerry UEM Cloud-Umgebung zu authentifizieren. Wenn Sie Ihre Umgebung mit einem lokalen BEMS konfigurieren, erlauben Sie iOS- und Android-Benutzern, zusätzlich zu den BEMS-Cloud-E-Mail-Benachrichtigungen für BlackBerry Work die Dienste Connect, Presence und Docs zu nutzen.

Hinweis: Sie können BEMS mit nur einer lokalen BlackBerry UEM oder einer BlackBerry UEM Cloud-Umgebung gleichzeitig konfigurieren.

Schritte zum Konfigurieren von BlackBerry UEM Cloud für die Kommunikation mit lokalen BEMS

Führen Sie die folgenden Aktionen aus, um BlackBerry UEM Cloud für die Kommunikation mit lokalen BEMS zu konfigurieren:

Hinweis: Einige der folgenden Aufgaben wurden möglicherweise bereits ausgeführt, als Sie BlackBerry UEM Cloud konfiguriert haben.

Schritt	Aktion
1	Konfigurieren Sie BlackBerry UEM Cloud in Ihrer Umgebung.
2	Installieren Sie in der BlackBerry UEM Cloud-Konsole den BlackBerry Connectivity Node oder führen Sie ein Upgrade auf die neueste Version durch. 1. Stellen Sie sicher, dass Ihr Unternehmen die Voraussetzungen für die Installation des BlackBerry Connectivity Node erfüllt 2. Laden Sie die Installations- und die Aktivierungsdateien für den BlackBerry Connectivity Node über die Verwaltungskonsole herunter 3. Installieren, aktivieren und konfigurieren Sie den BlackBerry Connectivity Node
3	Wenn Sie Connect und Docs verwenden, installieren und konfigurieren Sie die folgenden lokalen BEMS-Dienste. Weitere Anweisungen finden Sie in der Dokumentation zur BEMS-Installation in einer BlackBerry UEM-Umgebung und in der Dokumentation zur BEMS-Konfiguration in einer BlackBerry UEM-Umgebung. • BEMS-Connect • BEMS-Docs • BEMS-Presence

Schritt	Aktion
4	Konfigurieren des BlackBerry Dynamics-Server in BEMS im BEMS-Dashboard. Konfigurieren Sie optional die SSL-Kommunikation zwischen dem BlackBerry Connectivity Node und dem lokalen BEMS auf Port 17433. 1. Exportieren des BlackBerry Proxy-Zertifikats auf den lokalen Computer 2. Import des Zertifikats in den BEMS Windows-Schlüsselspeicher 3. Importieren des Zertifikats in den Java-Schlüsselspeicher auf BEMS **Hinweis:** Wenn Sie die SSL-Kommunikation nicht konfigurieren, deaktivieren Sie das Kontrollkästchen **SLL-Zertifikat-Validierung bei der Kommunikation mit BlackBerry Dynamics durchsetzen**.
5	Konfigurieren der BEMS-Konnektivität mit BlackBerry Dynamics im BEMS-Dashboard.

6	Weisen Sie Benutzern in der BlackBerry UEM Cloud-Konsole die Apps BlackBerry Connect, BlackBerry Presence-Dienst und Feature - Docs Service Entitlement zu.
	• Sie können die Apps mithilfe der folgenden Methoden zuweisen. Weitere Informationen finden Sie in der folgenden BlackBerry UEM Cloud-Dokumentation für Administratoren:
	  • Zuweisen einer App zu einer Benutzergruppe
	  • Zuweisen einer App-Gruppe zu einer Benutzergruppe
	  • Zuweisen einer App zu einem Benutzerkonto
	  • Zuweisen einer App oder App-Gruppe zu einem Benutzerkonto

7	Erstellen Sie in der BlackBerry UEM Cloud-Konsole ein BlackBerry Dynamics-Konnektivitätsprofil und fügen Sie den App-Server hinzu, auf dem die Apps BlackBerry Connect, BlackBerry Presence-Dienst und Feature - Docs Service Entitlement gehostet werden.

Import des Zertifikats in den BEMS Windows-Schlüsselspeicher

Damit der Connect-Dienst dem Zertifikat des BlackBerry Proxy-Servers vertraut, müssen Sie das BlackBerry Proxy-Zertifikat in den Connect-Dienst Windows-Schlüsselspeicher importieren. Wiederholen Sie diese Aufgabe auf jeder BEMS-Instanz.

Bevor Sie beginnen: Speichern Sie eine Kopie des ca.cer-Zertifikats, das Sie in einen geeigneten Speicherort auf dem Computer exportiert haben, der BEMS hostet. Anweisungen finden Sie unter Exportieren des BlackBerry Proxy-Zertifikats auf den lokalen Computer.

1. Öffnen Sie die Microsoft-Verwaltungskonsole.
2. Klicken Sie auf **Konsolenstamm**.
3. Klicken Sie auf **Datei > Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf **Zertifikate**.
5. Wählen Sie **Computerkonto > Lokaler Computer > OK**.
6. Erweitern Sie **Zertifikate (Lokaler Computer) > Vertrauenswürdige Stammzertifizierungsstellen**.
7. Klicken Sie mit der rechten Maustaste auf **Zertifikate** und klicken Sie auf **Alle Aufgaben > Importieren**.
8. Klicken Sie auf **Weiter**.

9. Navigieren Sie zum Speicherort des Zertifikats, das Sie exportiert haben (z. B. <*Laufwerk*>:\bemscert\ca.cer). Klicken Sie auf **Öffnen**.
10. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Fertigstellen**. Klicken Sie auf **OK**.

Wenn Sie fertig sind: Konfigurieren Sie den Core BEMS-Dienst für die Kommunikation mit BlackBerry Dynamics. Anweisungen finden Sie unter Konfigurieren der BEMS-Konnektivität mit BlackBerry Dynamics.

Importieren des Zertifikats in den Java-Schlüsselspeicher auf BEMS

Damit die Presence- und Docs-Dienste dem Zertifikat des BlackBerry Proxy-Servers vertrauen, müssen Sie das BlackBerry Connectivity Node-Zertifikat importieren. Verwenden Sie den DBmanager, um das Zertifikat in den BEMS Java-Schlüsselspeicher zu importieren. Standardmäßig befindet sich der DBmanager im Installationsordner unter <*Laufwerk*>:\GoodEnterpriseMobilityServer<*Version*>\GoodEnterpriseMobilityServer\DBManager.

Bevor Sie beginnen: Speichern Sie eine Kopie des ca.cer-Zertifikats, das Sie in einen geeigneten Speicherort auf dem Computer exportiert haben, der BEMS hostet. Anweisungen finden Sie unter Exportieren des BlackBerry Proxy-Zertifikats auf den lokalen Computer.

1. Prüfen Sie auf dem Computer, der das lokale BEMS hostet, dass die Systemvariable PATH den Pfad zum JAVA-Verzeichnis enthält.
   a) Geben Sie in einer Eingabeaufforderung `set | findstr "Path"` ein.
   b) Drücken Sie die **Eingabetaste**.

   Für weitere Informationen über das Festlegen der Path-System-Variable, siehe die Dokumentation zum „Konfigurieren der Java Runtime-Umgebung“ im BEMS in einer BlackBerry UEM-Umgebung.
2. Fertigen Sie eine Sicherungskopie der Java-Schlüsselspeicher-Datei an. Die Java-Schlüsselspeicher-Datei befindet sich unter `%JAVA_HOME%\lib\security\cacerts`, wo JAVA_HOME in Schritt 1 bestätigt wird.
3. Importieren Sie das Stamm-BlackBerry Proxy-Zertifikat.
   a) Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Ordner „DBManager“. Wenn die Installationsdateien z. B. im Ordner „Downloads“ gespeichert sind, geben Sie Folgendes ein: `C:\Users\besadmin\Downloads\GoodEnterpriseMobilityServer<Version>\GoodEnterpriseMobilityServer\DBManager`
   b) Importieren Sie das Zertifikat. Geben Sie Folgendes ein: `java -jar dbmanager-<Version>-jar-with-dependencies.jar -moduleName pushnotify -dbType sqlserver -dbName <SQL_Server_DB_Name> -dbHost <Name des Computers, der SQL DB hostet> -dbPort 1433 -userName gems_sa -password <BEMS_Dienst_Konto_Kennwort> -action addcertificate -pemFile "C:\<Pfad zum pemfile-Speicherort>\<Zertifikatsname>.cer" -alias gdcert`
4. Starten Sie den Good Technology Common Services-Dienst im Windows-Dienst-Manager neu.

Wenn Sie fertig sind: Konfigurieren Sie den Core BEMS-Dienst für die Kommunikation mit BlackBerry Dynamics. Anweisungen finden Sie unter Konfigurieren des BlackBerry Dynamics-Server in BEMS.

Konfigurieren des BlackBerry Dynamics-Server in BEMS

Ihre BEMS-Umgebung muss konfiguriert sein, um der Root-Zertifizierungsstelle für die BlackBerry Proxy-HTTPS-Konfiguration zu vertrauen oder die Karaf-Problemumgehung zu implementieren. Anweisungen hierzu finden Sie in der Dokumentation zum Importieren und Konfigurieren von Zertifikaten in der BEMS in einer BlackBerry UEM-Umgebung.

1. Klicken Sie im **BlackBerry Enterprise Mobility Server Dashboard** unter **BEMS System-Einstellungen** auf **BEMS Konfiguration**.
2. Klicken Sie auf **BlackBerry Dynamics**.
3. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Wenn ein BlackBerry Proxy-Server nicht definiert ist	**a.** Klicken Sie auf **BlackBerry Proxy hinzufügen**. **b.** Geben Sie im Feld **Hostname** den BlackBerry Proxy-Server-Hostnamen ein. **c.** Wählen Sie in der Drop-Down-Liste **Protokoll** das Protokoll aus, das verwendet wird, um mit dem BlackBerry Proxy-Server zu kommunizieren. • Wenn Sie HTTPS auswählen, wird das Feld **Port** mit 17433 ausgefüllt. Das ist sicher. • Wenn Sie HTTP auswählen, wird das Feld **Port** mit 17080 ausgefüllt. **Hinweis:** Wenn Sie Ihre Umgebung für HTTPS konfigurieren, müssen Sie Exportieren des BlackBerry Proxy-Zertifikats auf den lokalen Computer und dann Importieren des Zertifikats in den Java-Schlüsselspeicher auf BEMS. **d.** Klicken Sie auf **Test**, um die Verbindung zu testen. **e.** Wiederholen Sie die Schritte 1 bis 4, um weitere BlackBerry Proxy-Server für Zwecke der Redundanz hinzuzufügen.
Wenn ein oder mehrere BlackBerry Proxy-Server definiert sind	Es sind keine Maßnahmen erforderlich. Zuvor definierte BlackBerry Proxy-Server sind aufgelistet.

4. Klicken Sie auf das Kontrollkästchen **Auf andere Knoten im BEMS-Cluster anwenden**, um die BlackBerry Proxy-Server-Informationen an alle BEMS-Knoten im Cluster zu kommunizieren.
5. Wählen Sie optional das Kontrollkästchen **Die SLL-Zertifikat-Validierung bei der Kommunikation mit BlackBerry Dynamics durchsetzen**, wenn Sie das HTTPS-Protokoll verwenden, um mit dem BlackBerry Proxy-Server zu kommunizieren.
6. Klicken Sie auf **Speichern**.

Konfigurieren der BEMS-Konnektivität mit BlackBerry Dynamics

Bevor Sie beginnen: Stellen Sie sicher, dass die BlackBerry Control- und BlackBerry Proxy-Server installiert und in Betrieb sind. Weitere Informationen finden Sie in der Dokumentation zur Installation und zum Upgrade von BlackBerry UEM.

1. Klicken Sie im **BlackBerry Enterprise Mobility Server Dashboard** unter **BlackBerry Services Configuration** auf **Connect**.
2. Klicken Sie auf **Dienstkonto**.
3. Geben Sie den Benutzernamen und das Kennwort für das Dienstkonto ein.
4. Klicken Sie auf **Speichern**.

5. Klicken Sie auf **BlackBerry Dynamics**.
6. Geben Sie im Feld **Hostname** den BlackBerry Proxy-Serverhostnamen ein.
7. Die Portnummer wird im Feld **Port** auf der Grundlage der Kommunikation, die Sie ausgewählt haben, ausgefüllt.
   - Wenn Sie HTTP auswählen, wird das Feld „Port“ mit 17080 ausgefüllt.
   - Wenn Sie HTTPS auswählen, wird das Feld „Port“ mit 17433 ausgefüllt. Das ist sicher.

   Hinweis: Wenn Sie Ihre Umgebung für HTTPS konfigurieren, müssen Sie Exportieren des BlackBerry Proxy-Zertifikats auf den lokalen Computer und dann Import des Zertifikats in den BEMS Windows-Schlüsselspeicher.
8. Klicken Sie auf **Testen**, um die Verbindung zum BlackBerry Proxy-Server zu überprüfen.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Wenn Sie HTTPS ausgewählt haben, müssen Sie die BlackBerry Connect-App konfigurieren, um die SSL-Kommunikation nutzen zu können. Weitere Anweisungen finden Sie in der Dokumentation zu BlackBerry Connect für Administratoren unter „Konfigurieren von BlackBerry Connect-App-Einstellungen“ für Ihre Umgebung.

Hinzufügen eines App-Servers, der die Berechtigungs-Apps zu einem BlackBerry Dynamics-Konnektivitätsprofil hostet

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > BlackBerry Dynamics-Verbindungen**.
3. Klicken Sie auf +, um ein neues Konnektivitätsprofil zu erstellen, oder klicken Sie auf das BlackBerry Dynamics-Konnektivitätsprofil, für das Sie einen App-Server hinzufügen möchten.
4. Falls erforderlich, klicken Sie auf ✎.
5. Klicken Sie unter **App-Server** auf **Hinzufügen**.
6. Wählen Sie die App **Feature - Docs Service Entitlement**, für die Sie einen App-Server hinzufügen möchten.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie in der Tabelle für die App auf +.
9. Geben Sie im Feld **Server** den FQDN des lokalen BEMS-Servers an.
10. Geben Sie im Feld **Port** den Port des BlackBerry Proxy-Clusters an, der für den Zugriff auf den Server verwendet wird. Standardmäßig ist die Portnummer 8443.
11. Geben Sie in der Dropdown-Liste **Priorität** die Priorität dieses Servers oder dieser Server als primär an.
12. Geben Sie in der Dropdown-Liste **Primäres BlackBerry Proxy-Cluster** den Namen des BlackBerry Proxy-Clusters an, das Sie als primäres Cluster festlegen möchten.
13. Geben Sie in der Dropdown-Liste **Sekundäres BlackBerry Proxy-Cluster** den Namen des BlackBerry Proxy-Clusters an, das Sie als sekundäres Cluster festlegen möchten.
14. Klicken Sie auf **Speichern**.
15. Wiederholen Sie die Schritte 5 bis 14 für die folgenden Anwendungen:
    - BlackBerry Connect
    - BlackBerry Presence-Dienst

Exportieren des BlackBerry Proxy-Zertifikats auf den lokalen Computer

Wenn Sie die SSL-Kommunikation konfigurieren müssen, um die Kommunikation zwischen dem BlackBerry Connectivity Node und lokalen BEMS-Diensten zuzulassen (z. B. Connect-, Docs- und Mail-Dienste), exportieren Sie die BlackBerry Proxy-Stamm- und Zwischen-Zertifikatketten und importieren Sie sie in den Java-Schlüsselspeicher auf BEMS und den Windows-Schlüsselspeicher.

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

Bevor Sie beginnen: Überprüfen Sie, ob der BlackBerry Connectivity Node mit dem Status „Ausgeführt“ installiert ist.

1. Exportieren Sie auf dem Computer, der den BlackBerry Connectivity Node hostet, das BlackBerry Proxy-Zertifikat auf Ihren Computer. Geben Sie im Browser `https://localhost:17433` ein. Eine Zertifikatfehlermeldung wird angezeigt, weil das Zertifikat von einer Zertifizierungsstelle unterschrieben wurde, die nicht als bekannte Zertifizierungsstelle erkannt wurde.
2. Öffnen Sie das Dialogfeld „Zertifikat“ durch Klicken auf das Symbol „Zertifikat“ im URL-Feld.
3. Klicken Sie auf **Zertifikat**.
4. Klicken Sie auf **Certificate Path**.
5. Klicken Sie auf das Stammzertifikat. Das Stammzertifikat ist das erste Element in der Zertifikathierarchie.
6. Klicken Sie auf **Zertifikat anzeigen**.
7. Klicken Sie auf die Registerkarte **Details**.
8. Klicken Sie auf **In Datei kopieren**.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie **Base-64 encoded X.509 (.CER)**.
11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Durchsuchen**.
13. Geben Sie einen Namen für das Zertifikat ein (z. B. ca.cer) und exportieren Sie es auf den lokalen Computer.
14. Klicken Sie auf **Speichern**.
15. Klicken Sie auf **Fertigstellen**.
16. Klicken Sie auf **OK**.

Wenn Sie fertig sind:

- Wenn Sie den Connect-Dienst konfigurieren, kopieren Sie das exportierte BlackBerry Proxy-Zertifikat auf den Computer, der BEMS und Import des Zertifikats in den BEMS Windows-Schlüsselspeicher hostet.
- Wenn Sie den Presence-Dienst und den Docs-Dienst konfigurieren, kopieren Sie das exportierte BlackBerry Proxy-Zertifikat auf den Computer, der BEMS und Importieren des Zertifikats in den Java-Schlüsselspeicher auf BEMS hostet.

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 BlackBerry UEM-Quellserver migrieren.

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

Schritt	Aktion
1	Überprüfen Sie die Migrationsvoraussetzungen.
2	Herstellen einer Verbindung zu einem Quellserver.
3	Migrieren Sie optional IT-Richtlinien, Profilen und Gruppen.
5	Migrieren Sie Benutzer.
6	Migrieren Sie Geräte.

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

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

Voraussetzung	Details
Anmelden	Melden Sie sich bei BlackBerry UEM als Sicherheitsadministrator an.
Überprüfen der Softwareversion	Um Daten auf BlackBerry UEM zu migrieren, muss die BlackBerry UEM-Instanz, von der Sie Daten migrieren, über die neueste Version von BlackBerry UEM verfügen, einschließlich aller Wartungsversionen.
BlackBerry Connectivity Node	Aktivieren Sie mindestens eine BlackBerry Connectivity Node-Instanz.

Voraussetzung	Details
Konfigurieren der Verbindung mit dem BlackBerry UEM-Unternehmensverzeichnis	Konfigurieren Sie die Verbindung mit dem BlackBerry UEM-Zielunternehmensverzeichnis auf die gleiche Weise wie in der Quelle. Wenn die Quelle beispielsweise für die Active Directory-Integration konfiguriert und mit der Domäne „beispiel.com“ verbunden ist, konfigurieren Sie das BlackBerry UEM-Ziel für die Active Directory-Integration und die Verbindung mit der Domäne „beispiel.com“. **Wichtig:** Die Migration funktioniert nicht, wenn das Unternehmensverzeichnis auf dem Zielserver nicht mit dem Unternehmensverzeichnis auf dem Quellserver übereinstimmt.
Stellen Sie sicher, dass die erforderlichen Ports nicht durch eine Firewall blockiert werden.	Stellen Sie sicher, dass Port 8887 (TCP) auf BlackBerry Connectivity Node freigegeben ist. Stellen Sie sicher, dass Port 1433 (TCP) und Port 1434 (UDP) auf Microsoft SQL Server freigegeben sind.

Herstellen einer Verbindung zu einem Quellserver

Sie müssen eine Verbindung zwischen BlackBerry UEM und dem Quellserver herstellen, von dem aus Daten migriert werden.

Hinweis: Wenn mehr als ein BlackBerry Connectivity Node aktiviert ist, konfigurieren Sie unbedingt alle BlackBerry Connectivity Node-Instanzen, sodass eine Verbindung zur gleichen Quelldatenbank hergestellt wird.

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

1. Klicken Sie in der Menüleiste der BlackBerry Connectivity Node-Verwaltungskonsole auf **Allgemeine Einstellungen > Migration**.
2. Klicken Sie auf +.
3. Geben Sie im Feld **Anzeigename** einen beschreibenden Namen für die Quelldatenbank ein.
4. Geben Sie im Feld **Datenbankserver** den Namen des Computers ein, der die Quelldatenbank hostet. Verwenden Sie dabei für einen dynamischen Port das Format <Host>\<Instanz> und für einen statischen Port das Format <Host>:<Port>.
5. Wählen Sie in der Dropdown-Liste **Datenbank-Authentifizierungstyp** den Authentifizierungstyp aus, der für die Verbindung mit der Quelldatenbank verwendet werden soll.
6. Führen Sie einen der folgenden Schritte aus:

Option	Beschreibung
Bei Auswahl der SQL-Authentifizierung	a. Geben Sie in den Feldern **SQL-Benutzername** und **SQL-Kennwort** Ihre Anmeldeinformationen für die Verbindung mit der Quelldatenbank ein. b. Geben Sie im Feld **Datenbankname** den Namen der Quelldatenbank ein.

Option	Beschreibung
Bei Auswahl der Windows NT-Authentifizierung	**a.** Ändern Sie die Anmeldeeigenschaften des Diensts „BlackBerry UEM - BlackBerry Cloud Connector“, sodass sie auf dasselbe Konto verweisen, das auch zur Installation der BlackBerry UEM-Quelle verwendet wurde. Weitere Informationen zu Anmeldekonten finden Sie im Microsoft TechNet-Artikel zu Dienstberechtigungen. **Hinweis:** Nachdem die Migration von dieser Quelle aus abgeschlossen ist, legen Sie die Einstellung für die Anmeldeeigenschaften wieder auf das lokale Systemkonto fest. **b.** Geben Sie im Feld **Datenbankname** den Namen der Quelldatenbank ein.

7. Klicken Sie auf **Speichern**.
8. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Einstellungen > Migration > Konfiguration**.
9. Klicken Sie auf +.
10. Geben Sie den Anzeigenamen der Quelldatenbank ein, die Sie in der BlackBerry Connectivity Node-Verwaltungskonsole konfiguriert haben.
11. Klicken Sie auf **Speichern**.
12. Klicken Sie zum Testen der Verbindung zwischen der Quelle und dem Ziel auf **Verbindung testen**.

Wenn Sie fertig sind:

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

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

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

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

BlackBerry UEM

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

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

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

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

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie auf **Migration** > **IT-Richtlinien, Profile, Gruppen**.
3. Klicken Sie auf **Weiter**.
4. Aktivieren Sie die Kontrollkästchen für die Elemente, die Sie migrieren möchten.

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

Wenn Sie fertig sind: Erstellen Sie auf dem Zielserver die Richtlinien und Profile, die nicht migriert werden konnten, und weisen Sie sie den Benutzern vor der Migration von Geräten zu.

Überlegungen: Migrieren von Benutzern aus einem Quellserver

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

Objekt	Überlegungen
Maximale Anzahl für die Migration	Sie können maximal 1000 Benutzer gleichzeitig aus einer Quelle migrieren. Wenn Sie mehr als die maximale Anzahl Benutzer für die Migration auswählen, wird nur die maximale Anzahl Benutzer in das BlackBerry UEM-Ziel migriert. Die verbleibenden Benutzer werden ausgelassen. Wiederholen Sie den Migrationsvorgang so häufig wie nötig, um alle Benutzer aus dem Quellserver zu migrieren. **Hinweis:** Wenn BlackBerry UEM das Zeitlimit während der Migration von 1000 Benutzern überschreitet, versuchen Sie die Migration mit weniger Benutzern.
E-Mail-Adresse	• Benutzer benötigen eine E-Mail-Adresse, bevor die Migration erfolgen kann. • Benutzer, die eine im BlackBerry UEM-Ziel bereits vorhandene E-Mail-Adresse verwenden, können nicht migriert werden. Diese Benutzer erscheinen nicht in der Liste der zu migrierenden Benutzer. • Wenn zwei Benutzer in der Quelle die gleiche E-Mail-Adresse haben, wird nur ein Benutzer auf dem Bildschirm „Migrieren von Benutzern“ angezeigt. • Wenn zwei Benutzer in der Quelle die gleiche E-Mail-Adresse aufweisen, können die auf dem Bildschirm „Migrieren von Geräten“ angezeigten Benutzerinformationen entweder von dem einen oder dem anderen Benutzer stammen.
Kennwort	Nach der Migration müssen lokale Benutzer nach dem ersten Anmelden bei BlackBerry UEM Self-Service Ihr Kennwort ändern. Benutzer, die vor der Migration keine Zugriffsberechtigung für BES12 Self-Service oder BlackBerry UEM Self-Service hatten, erhalten nach der Migration nicht automatisch Berechtigung.
Gruppen	Sie können Benutzer ohne Gruppenzuordnung filtern, um diese Benutzergruppe bei einer Migration mit aufzunehmen.

Migrieren von Benutzern aus einem Quellserver

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Migration > Benutzer**.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie die zu migrierenden Benutzer aus.
4. Klicken Sie auf **Weiter**.
5. Weisen Sie den ausgewählten Benutzern mindestens eine Gruppe, eine IT-Richtlinie und mindestens ein Profil zu.

Weitere Informationen finden Sie in der Dokumentation für Administratoren.

6. Klicken Sie auf **Vorschau**.
7. Klicken Sie auf **Migrieren**.

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

Überlegungen: Migrieren von Geräten aus einem Quellserver

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

Objekt	Überlegungen
Maximale Anzahl für die Migration	Sie können maximal 2000 Geräte gleichzeitig aus einem Quellserver migrieren.
Ziel-BlackBerry UEM	Überprüfen Sie vor der Migration von Geräten, ob BlackBerry UEM den Gerätetyp und das Betriebssystem unterstützt.
Benutzer	• Die Benutzer müssen in der BlackBerry UEM-Zieldomäne vorhanden sein. • Für Migrationen von BlackBerry UEM können Sie pro Benutzer nicht mehr als fünf Geräte gleichzeitig migrieren.
iOS-Geräte	• Auf den iOS-Geräten muss die aktuelle Version von BlackBerry UEM Client installiert sein. • Alle iOS-Geräte müssen vertrauenswürdig sein (nicht vertrauenswürdige iOS-Geräte können nicht migriert werden). • iOS-Geräte, denen das App-Sperrprofil zugewiesen ist, können nicht migriert werden, weil BlackBerry UEM Client nicht für die Migration geöffnet werden kann.
Android-Geräte	• Auf den Android-Geräten muss die aktuelle Version von BlackBerry UEM Client installiert sein. • Sie können Android-Geräte, die ein Arbeitsprofil haben, nicht migrieren.
Windows-Geräte	Windows-Geräte können nicht migriert werden.
macOS-Geräte	macOS-Geräte können nicht migriert werden.
MDM-Steuerelemente	Geräte, die über „MDM-Steuerelemente“ aktiviert wurden, können vorübergehend nicht auf E-Mails zugreifen, wenn die Migration beginnt. Der E-Mail-Dienst wird wiederhergestellt, wenn die Migration abgeschlossen ist.

Migrieren von Geräten aus einem Quellserver

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

Bevor Sie beginnen:

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Migration > Geräte**.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie die zu migrierenden Geräte aus.
4. Klicken Sie auf **Vorschau**.
5. Klicken Sie auf **Migrieren**.
6. Um den Status der zu migrierenden Geräte anzuzeigen, klicken Sie auf **Migration** > **Status**.

Kurzanleitung für Gerätemigration

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

Migrieren von DEP-Geräten

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

Migrieren von DEP-Geräten mit installiertem BlackBerry UEM Client

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

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

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

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

Migrieren von DEP-Geräten ohne BlackBerry UEM Client

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

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

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

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada