



# **BlackBerry UEM for dark sites**

## **Installation and Administration Guide**

12.17



# Inhalt

<b>Informationen über BlackBerry UEM für Dark Sites.....</b>	<b>4</b>
Unterstützte BlackBerry UEM-Funktionen.....	4
Nicht unterstützte BlackBerry UEM-Funktionen.....	4
Architektur: BlackBerry UEM für Dark Sites.....	6
<b>Installation oder Upgrade von BlackBerry UEM in einer Dark-Site- Umgebung.....</b>	<b>8</b>
Installieren oder Aktualisieren von BlackBerry UEM.....	8
Anmelden bei BlackBerry UEM.....	9
Erstmalige Anmeldung bei BlackBerry UEM.....	9
<b>Konfigurieren von BlackBerry UEM für Dark Sites.....</b>	<b>10</b>
Hinzufügen von Lizenzen zu BlackBerry UEM.....	11
Importieren von BlackBerry UEM-Lizenzen.....	11
Festlegen von Samsung Knox-Lizenzschlüsseln.....	12
Abrufen eines APNs-Zertifikats für die Verwaltung von iOS-Geräten.....	12
Abrufen einer signierten CSR-Datei von BlackBerry.....	12
Anfordern eines APNs-Zertifikats von Apple.....	13
Registrieren des APNs-Zertifikats.....	13
<b>Verwalten von Benutzern und Geräten in einer Dark-Site-Umgebung.....</b>	<b>14</b>
Geräteaktivierung.....	14
Unterstützte Aktivierungsarten.....	14
Vorbereiten von Benutzern auf die Aktivierung von Geräten.....	17
Aktivieren von BlackBerry 10-Geräten.....	20
Aktivieren von Samsung Knox-Geräten.....	24
Aktivieren von iOS-Geräten.....	29
Verwalten von BlackBerry 10-Geräten.....	31
Verwalten von Samsung Knox-Geräten.....	31
Einrichten des VPNs mit Knox StrongSwan.....	32
Verwalten von iOS-Geräten.....	32
<b>Produktdokumentation.....</b>	<b>34</b>
<b>Rechtliche Hinweise.....</b>	<b>35</b>

# Informationen über BlackBerry UEM für Dark Sites

BlackBerry UEM ist eine plattformübergreifende EMM-Lösung von BlackBerry, die umfassende Funktionen für die Verwaltung von Geräten und Anwendungen sowie für das Content Management mit integrierter Sicherheit und Konnektivität bietet.

In Umgebungen mit höchsten Sicherheitsanforderungen ist die Herstellung einer Verbindung mit externen Standorten wie der BlackBerry Infrastructure möglicherweise eingeschränkt oder nicht möglich. BlackBerry UEM für Dark Sites wurde entwickelt, um eine sichere Verwaltungslösung für mobile Geräte bereitzustellen, ohne dass BlackBerry UEM eine Verbindung mit der BlackBerry Infrastructure und anderen Diensten im Internet herstellen muss.

## Unterstützte BlackBerry UEM-Funktionen

Die folgenden BlackBerry UEM-Funktionen werden in einer Dark-Site-Umgebung unterstützt.

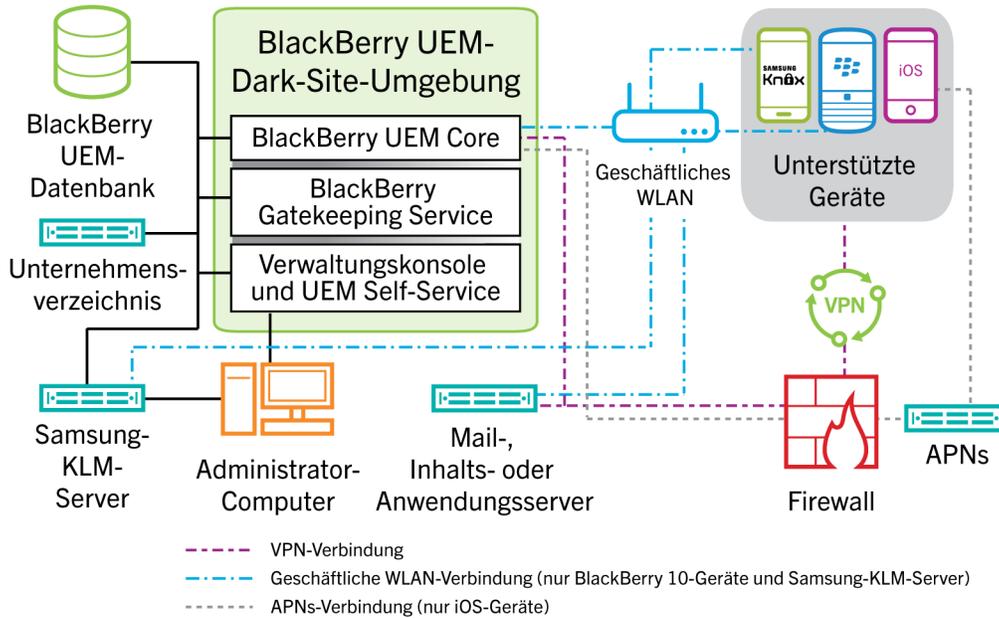
Funktion	Beschreibung
Plattformübergreifende Geräteverwaltung	Sie können BlackBerry 10-, iOS- und Samsung Knox-Geräte verwalten.
Zuverlässige und sichere Benutzererfahrung	Steuerungsfunktionen für Geräte ermöglichen eine präzise Verwaltung der Verbindung von Geräten mit dem Netzwerk, der aktivierten Funktionen und der verfügbaren Apps.
Steuern des Zugriffs auf Microsoft Exchange	Ihr Unternehmen kann mit BlackBerry Gatekeeping Service steuern, welche Geräte Zugriff auf Exchange ActiveSync erhalten. Alle Geräte, die nicht in der Positivliste für Microsoft Exchange aufgeführt sind, werden in der UEM-Liste der eingeschränkten Exchange ActiveSync-Geräte erfasst, und ihr Zugriff auf geschäftliche E-Mail- und Terminplanerdaten wird blockiert.
App-Verwaltung	Sie können interne Apps auf Geräten installieren und verwalten. Sie können außerdem verhindern, dass Geräte Apps aus anderen Quellen installieren können.
Rollenbasierte Verwaltung	Sie können Verwaltungsaufgaben für andere Administratoren freigeben, die gleichzeitig auf die Administrationskonsolen zugreifen können. Sie können mithilfe von Rollen die Aktionen definieren, die ein Administrator ausführen kann, und durch die Beschränkung der Optionen für die einzelnen Administratoren Sicherheitsrisiken senken, Aufgaben verteilen und die Effizienz erhöhen. Sie können vordefinierte Rollen verwenden oder eigene Rollen erstellen.

## Nicht unterstützte BlackBerry UEM-Funktionen

Die folgenden BlackBerry UEM-Funktionen werden in einer Dark-Site-Umgebung nicht unterstützt. Diese Funktionen sind in BlackBerry UEM für Dark Sites deaktiviert.

Nicht unterstützte Funktionen	Erläuterung
Geräte	BlackBerry UEM für Dark Sites unterstützt nur BlackBerry 10-, iOS- und Samsung-Geräte.
Enterprise-Konnektivität	<p>BlackBerry UEM-Funktionen, die zulassen, dass Geräte über die BlackBerry Infrastructure eine Verbindung mit Ressourcen Ihrer Organisation herstellen, werden nicht unterstützt, darunter die folgenden:</p> <ul style="list-style-type: none"> <li>• BlackBerry Secure Connect Plus</li> <li>• BlackBerry Secure Gateway</li> <li>• BlackBerry MDS Connection Service</li> <li>• Verwenden von BlackBerry UEM als Proxy für SCEP-Anforderungen</li> </ul>
BlackBerry Dynamics	BlackBerry Dynamics-Apps, einschließlich BlackBerry Work, werden nicht unterstützt.
Weitere BlackBerry-Enterprise-Produkte	<p>BlackBerry UEM für Dark Sites arbeitet nicht mit anderen BlackBerry-Enterprise-Produkten zusammen, darunter die folgenden:</p> <ul style="list-style-type: none"> <li>• BlackBerry Enterprise Identity</li> <li>• BlackBerry 2FA</li> </ul>
Verwaltung öffentlicher Apps und Apps, die von Microsoft Intune geschützt werden	<p>BlackBerry UEM für Dark Sites bietet keine Unterstützung für Verbindungen mit Anbietern öffentlicher Apps wie BlackBerry World, Apple App Store und Google Play. Sie können keine öffentlichen Apps zu den Geräten von Benutzern hinzufügen.</p> <p>BlackBerry UEM für Dark Sites unterstützt keine Verbindungen mit Microsoft Azure. Sie können Apps nicht mit Microsoft Intune-App-Schutzprofile verwalten.</p>

# Architektur: BlackBerry UEM für Dark Sites



Komponentenname	Beschreibung
BlackBerry UEM Core	<p>BlackBerry UEM Core ist die zentrale Komponente der BlackBerry UEM-Architektur. Er weist mehrere Unterkomponenten auf, die verantwortlich sind für:</p> <ul style="list-style-type: none"> <li>• Protokollierung, Überwachung, Reporting und Verwaltungsfunktionen</li> <li>• Authentifizierungs- und Autorisierungsdienste</li> <li>• Planen und Senden von Befehlen, IT-Richtlinien und Profilen an Geräte</li> </ul>
BlackBerry UEM-Datenbank	<p>Die BlackBerry UEM-Datenbank ist eine relationale Datenbank, die Informationen zum Benutzerkonto und der Konfiguration enthält, die von BlackBerry UEM für die Verwaltung von Geräten verwendet werden.</p>
BlackBerry Gatekeeping Service	<p>Der BlackBerry Gatekeeping Service sendet Befehle an Exchange ActiveSync, um Geräte einer Positivliste hinzuzufügen, wenn Geräte auf BlackBerry UEM aktiviert werden. Nicht verwaltete Geräte, die versuchen, sich mit einem E-Mail-Server des Unternehmens zu verbinden, können durch einen Administrator über die BlackBerry UEM-Verwaltungskonsole überprüft, verifiziert und blockiert oder zugelassen werden.</p>
Verwaltungskonsole und UEM Self-Service	<p>Die Verwaltungskonsole und der UEM Self-Service bilden eine browserbasierte Benutzerschnittstelle, die Administrator- und Benutzerzugriff auf BlackBerry UEM ermöglicht.</p> <p>Sie können Systemeinstellungen, Benutzer, Geräte und Apps über die Verwaltungskonsole verwalten.</p> <p>Benutzer können den UEM Self-Service verwenden, um ein Aktivierungskennwort einzurichten und Befehle, z. B. zum Einrichten des Kennworts, Sperren des Geräts und Löschen von Gerätedaten, an Geräte zu senden.</p>

Komponentenname	Beschreibung
Mail-, Inhalts- oder Anwendungsserver	<p>Ihr internes Netzwerk umfasst verschiedene Dienste, mit denen Geräte und BlackBerry UEM kommunizieren können.</p> <p>Wenn Sie Samsung Knox-Geräte mithilfe von Aktivierungsarten für Android Enterprise aktivieren, benötigen Sie einen Server, der die APK-Datei für den BlackBerry UEM Client enthält und eine PAC-Datei, die verhindert, dass Geräte versuchen, während der Aktivierung eine Verbindung zu Google Play herzustellen.</p>
Samsung-KLM-Server	<p>Wenn Sie Samsung Knox-Geräte verwalten, wird ein Samsung Knox-Lizenzverwaltungsserver mit BlackBerry UEM für Dark Sites installiert, damit BlackBerry UEM keine Verbindung zum webbasierten Samsung Knox-Lizenzverwaltungssystem herstellen muss, um Lizenzinformationen abzurufen.</p> <p>Samsung Knox-Geräte kommunizieren mit dem KLM-Server über das geschäftliche Wi-Fi-Netzwerk.</p>
APNs	<p>Zum Verwalten von iOS-Geräten muss BlackBerry UEM Benachrichtigungen über einen APNs-Server an Geräte senden. Wenn Geräte eine Benachrichtigung von APNs erhalten, stellen sie für die Suche nach Updates eine Verbindung zu BlackBerry UEM her.</p> <p>Informationen zum Sichern von Verbindungen mit APNs oder zu möglichen Alternativen zur Verwendung der öffentlichen APNs erhalten Sie von einem Apple-Supportmitarbeiter.</p>

# Installation oder Upgrade von BlackBerry UEM in einer Dark-Site-Umgebung

Bei der Installation von BlackBerry UEM in einer Dark-Site-Umgebung werden nur die folgenden Komponenten aktiviert:

- BlackBerry UEM-Verwaltungskonsole
- BlackBerry UEM Core
- BlackBerry Gatekeeping Service

Sie können für BlackBerry UEM ein Upgrade durchführen. Informationen zum Migrieren von Geräten zu einer neuen BlackBerry UEM-Umgebung [finden Sie in der BlackBerry UEM Dokumentation zur Konfiguration](#).

Wenn Sie BlackBerry UEM installieren oder upgraden, können Sie einen vorhandenen Microsoft SQL Server oder Microsoft SQL Server Express installieren und verwenden.

**Hinweis:** Prüfen Sie vor der Installation oder dem Upgrade von BlackBerry UEM die Anforderungen und Voraussetzungen in der [BlackBerry UEM-Dokumentation zur Planung](#) und in der [Dokumentation zu Installation und Upgrade](#). Die Port-Anforderungen sind in der [Dokumentation zur Planung enthalten](#).

## Installieren oder Aktualisieren von BlackBerry UEM

1. Melden Sie sich als Benutzer mit lokalen Administratorrechten bei dem Server an, auf dem Sie BlackBerry UEM installieren oder aktualisieren möchten.
2. Laden Sie die BlackBerry UEM-Installationsdateien herunter, und extrahieren Sie sie.
3. Ändern Sie die Datei „deployer.properties“ mit den Parametern für Ihre Umgebung. Die Datei „deployer.properties“ befindet sich im selben Ordner wie die Datei „setup.exe“.
  - a) Geben Sie im Feld **service.account.password=** das Kennwort für das Konto ein, mit dem Sie angemeldet sind.
  - b) Wenn Sie einen vorhandenen Microsoft SQL Server verwenden möchten, geben Sie die Informationen in die entsprechenden Felder für diesen Server ein.

Informationen zum Ausfüllen der Felder finden Sie unter [deployer.properties-Datei](#) in der BlackBerry UEM-Dokumentation zu Installation und Upgrade.

4. Öffnen Sie als Administrator ein Eingabeaufforderungsfenster, und geben Sie in dem Verzeichnis, in dem Sie die BlackBerry UEM-Installationsdateien extrahiert haben, einen der folgenden Befehle ein:

Option	Befehl
Zur Verwendung einer vorhandenen Microsoft SQL Server-Datenbank	<pre>setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog</pre>
Zur Installation einer lokalen Microsoft SQL Server-Datenbank	<pre>setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog --installSQL</pre>

# Anmelden bei BlackBerry UEM

Melden Sie sich nach der Installation von BlackBerry UEM bei der Verwaltungskonsole an.

**Hinweis:** Wenn Sie sich erstmals bei BlackBerry UEM anmelden, müssen Sie neben dem Namen Ihrer Organisation, dem SRP-Bezeichner und dem SRP-Authentifizierungsschlüssel den **Namen der Lizenzdatei** eingeben. Sie erhalten die Lizenzdatei von einem BlackBerry-Vertriebsmitarbeiter. Der SRP-Bezeichner und der SRP-Authentifizierungsschlüssel müssen mit den Informationen in der Lizenzdatei übereinstimmen.



**VORSICHT:** Verwenden Sie nicht die SRP-ID aus früheren BES5-, BES10-, BES12- oder BlackBerry UEM-Instanzen, wenn Sie eine neue Instanz von BlackBerry UEM installieren.

## Erstmalige Anmeldung bei BlackBerry UEM

**Bevor Sie beginnen:** Stellen Sie sicher, dass Sie den Namen des Unternehmens, die SRP-ID und den SRP-Authentifizierungsschlüssel für BlackBerry UEM kennen.

Wenn die Setupanwendung weiterhin geöffnet ist, können Sie direkt über das Dialogfenster „Konsolenadresse“ auf die Verwaltungskonsole zugreifen.

1. Geben Sie in die Adresszeile des Browsers **https://<server\_name>:<port>/admin** ein; dabei steht <server\_name> für den FQDN des Computers, der die Verwaltungskonsole hostet. Der Standardport der Verwaltungskonsole lautet „Port 443“.
2. Geben Sie in das Feld **Benutzername** den Wert **admin** ein.
3. Geben Sie in das Feld **Kennwort** den Wert **password** ein.
4. Klicken Sie auf **Anmelden**.
5. Wählen Sie in der Dropdown-Liste „Serverstandort“ das Land des Computers aus, auf dem BlackBerry UEM installiert ist, und klicken Sie auf **Weiter**.
6. Geben Sie den Namen Ihres Unternehmens, die SRP-ID und den SRP-Authentifizierungsschlüssel ein.
7. Klicken Sie auf **Submit**.
8. Ändern Sie das temporäre Kennwort in ein dauerhaftes Kennwort.
9. Klicken Sie auf **Submit**.

### Wenn Sie fertig sind:

- Bei der Anmeldung an der Verwaltungskonsole können Sie sich entscheiden, ob Sie den Bildschirm zu **Willkommen zu BlackBerry UEM** ansehen oder schließen möchten. Wenn Sie das Dialogfeld schließen, wird es während der nächsten Anmeldungen nicht mehr angezeigt.

# Konfigurieren von BlackBerry UEM für Dark Sites

In der folgenden Tabelle sind die Konfigurationsaufgaben zusammengefasst, die Sie möglicherweise nach der Installation von BlackBerry UEM in einer Dark-Site-Umgebung durchführen müssen.

Weitere Informationen zum Konfigurieren von BlackBerry UEM finden Sie in der [BlackBerry UEM Dokumentation zur Konfiguration](#).

Aufgabe	Beschreibung
BlackBerry UEM-Lizenzdatei importieren	<p>In einer Dark-Site-Umgebung müssen Sie Lizenzinformationen manuell in BlackBerry UEM importieren.</p> <p>Weitere Informationen finden Sie unter <a href="#">Hinzufügen von Lizenzen zu BlackBerry UEM</a>.</p>
Standardzertifikate durch vertrauenswürdige Zertifikate ersetzen	<p>Sie können das SSL-Standardzertifikat, das von den BlackBerry UEM-Konsolen verwendet wird, sowie das Standardzertifikat, das von BlackBerry UEM zum Signieren des MDM-Profiles für iOS-Geräte verwendet wird, durch vertrauenswürdige Zertifikate ersetzen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Ändern von BlackBerry UEM-Zertifikaten</a> in der Dokumentation zur BlackBerry UEM-Konfiguration.</p>
Konfigurieren von Verbindungen über interne Proxyserver	<p>Wenn Ihr Unternehmen einen Proxyserver für Verbindungen zwischen den Servern in Ihrem Netzwerk nutzt, müssen Sie die serverseitigen Proxyeinstellungen möglicherweise so konfigurieren, dass BlackBerry UEM Core mit Remote-Instanzen der Verwaltungskonsole kommunizieren kann.</p> <p>Weitere Informationen finden Sie unter <a href="#">Konfigurieren von Verbindungen über interne Proxyserver</a> in der Dokumentation zur BlackBerry UEM-Konfiguration.</p>
Verbindung zwischen BlackBerry UEM und Unternehmensverzeichnissen herstellen	<p>Sie können BlackBerry UEM mit einem oder mehreren Unternehmensverzeichnissen verbinden, damit BlackBerry UEM zum Erstellen von Benutzerkonten auf Benutzerdaten zugreifen kann.</p> <p>Weitere Informationen finden Sie unter <a href="#">Herstellen einer Verbindung mit Ihren Unternehmensverzeichnissen</a> in der Dokumentation zur BlackBerry UEM-Konfiguration.</p>
Verbindung zwischen BlackBerry UEM und einem SMTP-Server herstellen	<p>Wenn Sie möchten, dass BlackBerry UEM Aktivierungs-E-Mails und andere Benachrichtigungen an Benutzer sendet, müssen Sie die Einstellungen für den SMTP-Server festlegen, den BlackBerry UEM verwenden kann.</p> <p>Weitere Informationen finden Sie unter <a href="#">Herstellen einer Verbindung mit einem SMTP-Server zum Senden von E-Mail-Benachrichtigungen</a> in der Dokumentation zur BlackBerry UEM-Konfiguration.</p>

Aufgabe	Beschreibung
APNs-Zertifikat abrufen und registrieren	<p>Wenn Sie iOS-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.</p> <p>Weitere Informationen finden Sie unter <a href="#">Abrufen eines APNs-Zertifikats für die Verwaltung von iOS-Geräten</a>.</p>
Steuern, welche Geräte Zugriff auf Exchange ActiveSync erhalten	<p>Wenn Sie Microsoft Exchange konfiguriert haben, damit Geräte nicht auf geschäftliche E-Mail- und Terminplanerdaten zugreifen können, sofern die Geräte nicht zu einer Liste zulässiger Geräte hinzugefügt wurden, müssen Sie eine Microsoft Exchange-Konfiguration in BlackBerry UEM erstellen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Steuern, welche Geräte Zugriff auf Exchange ActiveSync erhalten</a> in der Dokumentation für BlackBerry UEM-Administratoren.</p>
Einrichtung der BlackBerry UEM Self-Service	<p>Wenn Sie die Ausführung bestimmter Verwaltungsaufgaben durch Benutzer zulassen möchten, z. B. Ändern von Kennwörtern, können Sie die BlackBerry UEM Self-Service-Webanwendung einrichten und verteilen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Einrichten von BlackBerry UEM Self-Service für Benutzer</a> in der Dokumentation für BlackBerry UEM-Administratoren.</p>

## Hinzufügen von Lizenzen zu BlackBerry UEM

Wenn BlackBerry UEM in einer Dark-Site-Umgebung installiert ist, müssen Lizenzinformationen manuell in BlackBerry UEM importiert werden.

Wenn Sie Samsung Knox-Geräte verwalten, müssen Sie außerdem die Samsung Knox-ELM- und KLM-Lizenzschlüssel festlegen.

Um eine manuelle Aktualisieren von Lizenzen in der Zukunft zu vermeiden, insbesondere für Samsung Knox-Geräte, sollten Sie unbefristete Lizenzen für die Dark-Site-Umgebung Ihres Unternehmens erwerben.

Sie erhalten eine BlackBerry UEM-Lizenzdatei und die Samsung-Lizenzschlüssel von einem BlackBerry-Vertriebsmitarbeiter.

### Importieren von BlackBerry UEM-Lizenzen

**Bevor Sie beginnen:** Erwerben Sie eine BlackBerry UEM-Lizenzdatei von einem BlackBerry-Vertriebsmitarbeiter.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Lizenzierung**.
2. Klicken Sie auf der Seite **Lizenzübersicht** auf **Lizenz importieren**.  
Wenn Sie die vorhandenen Lizenzen aktualisieren möchten, klicken Sie stattdessen auf **Lizenzen aktualisieren**.
3. Klicken Sie auf **Durchsuchen**.
4. Wählen Sie die zu verwendende Lizenzdatei aus.
5. Klicken Sie auf **Öffnen**.

## Festlegen von Samsung Knox-Lizenzschlüsseln

Wenn Sie Samsung Knox-Geräte in einer Dark-Site-Umgebung verwalten, müssen Sie Samsung Knox-Lizenzschlüssel in BlackBerry UEM festlegen.

**Bevor Sie beginnen:** Sie erhalten Samsung Knox-ELM- und KLM-Lizenzschlüssel von einem BlackBerry-Vertriebsmitarbeiter.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Lizenzierung**.
2. Klicken Sie auf der Seite **Lizenzübersicht** auf **KNOX-Lizenzschlüssel einrichten**.
3. Fügen Sie den Samsung Knox-ELM- und den Samsung Knox-KLM-Lizenzschlüssel in die entsprechenden Felder ein.
4. Klicken Sie auf **Speichern**.

## Abrufen eines APNs-Zertifikats für die Verwaltung von iOS-Geräten

APNs ist der Apple Push Notification Service. Die Verwaltung von iOS-Geräten setzt voraus, dass BlackBerry UEM eine Verbindung mit dem APNs von Apple herstellen kann. Informationen zum Sichern von Verbindungen mit APNs oder zu möglichen Alternativen zur Verwendung der öffentlichen APNs erhalten Sie von einem Apple-Supportmitarbeiter.

Sie müssen ein APNs-Zertifikat abrufen und registrieren, das BlackBerry UEM für die Verwaltung von iOS-Geräten verwenden soll.

**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. 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- 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 für öffentliche APNs die folgenden Aktionen aus:

Schritt	Aktion
1	Abrufen einer signierten CSR-Datei von BlackBerry.
2	Fordern Sie mit der signierten CSR-Datei ein APNs-Zertifikat von Apple an.
3	Registrieren des APNs-Zertifikats.

### Abrufen einer signierten CSR-Datei von BlackBerry

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

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Apple Push Notification**.
2. Klicken Sie auf **APNs-Zertifikat abrufen**.  
Wenn Sie ein aktuell verwendetes APNs-Zertifikat erneuern möchten, klicken Sie stattdessen auf **Zertifikat erneuern**.
3. Klicken Sie im Abschnitt **Schritt 1 von 3 – Signiertes CSR-Zertifikat von BlackBerry herunterladen** auf **Signaturanforderung für Zertifikat herunterladen**.
4. Klicken Sie auf **Speichern**, um die unsignierte CSR-Datei (.scsr) auf Ihrem Computer zu speichern.
5. Senden Sie die unsignierte CSR-Datei an einen BlackBerry-Kundensupportmitarbeiter.  
Der Kundensupportmitarbeiter lässt die CSR-Datei von einer BlackBerry-Zertifizierungsstelle signieren und sendet die signierte CSR-Datei an Sie zurück.

**Wenn Sie fertig sind:** [Anfordern eines APNs-Zertifikats von Apple](#).

## **Anfordern eines APNs-Zertifikats von Apple**

**Bevor Sie beginnen:** [Abrufen einer signierten CSR-Datei von BlackBerry](#).

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

**Wenn Sie fertig sind:** [Registrieren des APNs-Zertifikats](#).

## **Registrieren des APNs-Zertifikats**

**Bevor Sie beginnen:** [Anfordern eines APNs-Zertifikats von Apple](#).

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

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

# Verwalten von Benutzern und Geräten in einer Dark-Site-Umgebung

Die Aufgaben für die Benutzer- und Geräteverwaltung sind für die meisten unterstützten Funktionen in einer Dark-Site-Umgebung identisch mit denen in jeder anderen BlackBerry UEM-Umgebung. Anweisungen zu den meisten administrativen Aufgaben, die in diesem Dokument nicht abgedeckt sind, [finden Sie in der BlackBerry UEM-Dokumentation zur Administration](#).

## Geräteaktivierung

Wenn Sie ein Gerät aktivieren, verknüpfen Sie das Gerät mit BlackBerry UEM, damit Sie das Gerät verwalten und Benutzer auf geschäftliche Daten auf dem Gerät zugreifen können.

Wenn ein Gerät aktiviert wurde, können Sie IT-Richtlinien und Profile versenden, um die verfügbaren Funktionen zu überwachen und die Sicherheit der geschäftlichen Daten sicherzustellen. Sie können auch Apps zuweisen, die der Benutzer installieren kann. Je nachdem, wie viel Kontrolle die ausgewählte Aktivierungsart zulässt, können Sie das Gerät auch dadurch schützen, dass Sie den Zugriff auf bestimmte Daten einschränken, dezentral Kennwörter festlegen, das Gerät sperren oder Daten löschen.

### Unterstützte Aktivierungsarten

BlackBerry UEM für Dark Sites unterstützt die folgenden Aktivierungsarten für BlackBerry 10-, Samsung Knox- und iOS-Geräte.

#### BlackBerry 10-Geräte

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Unternehmen	<p>Diese Aktivierungsart ermöglicht die Steuerung von geschäftlichen Daten auf Geräten und stellt gleichzeitig sicher, dass private Daten geschützt werden. Wenn ein Gerät aktiviert wird, wird auf dem Gerät ein separater geschäftlicher Bereich erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Alle geschäftlichen Daten von vorherigen Aktivierungen werden gelöscht.</p> <p>Mithilfe von Befehlen und IT-Richtlinien können Sie den geschäftlichen Bereich des Geräts steuern, jedoch nicht den persönlichen Bereich des Geräts.</p>
Nur geschäftlicher Bereich	<p>Diese Aktivierungsart ermöglicht eine vollständige Kontrolle über die Geräte und bietet keinen separaten Bereich für persönliche Daten. Wenn ein Gerät aktiviert wird, werden der persönliche Bereich sowie alle geschäftlichen Daten von vorherigen Aktivierungen entfernt, und es wird ein geschäftlicher Bereich erstellt. Der Benutzer muss ein Kennwort einrichten, um auf das Gerät zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt.</p> <p>Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern.</p>

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – Reguliert	<p>Diese Aktivierungsart ermöglicht die Kontrolle über die geschäftlichen und die persönlichen Daten. Wenn ein Gerät aktiviert wird, wird auf dem Gerät ein separater geschäftlicher Bereich erstellt, und der Benutzer muss ein Kennwort erstellen, um auf den geschäftlichen Bereich zuzugreifen. Geschäftsdaten werden über Verschlüsselung und Kennwortauthentifizierung geschützt. Alle geschäftlichen Daten von vorherigen Aktivierungen werden gelöscht.</p> <p>Sie können sowohl den geschäftlichen als auch den persönlichen Bereich auf dem Gerät mit Befehlen und IT-Richtlinien steuern.</p>

### Samsung Knox-Geräte

**Hinweis:** Samsung Knox-Aktivierungsarten werden in einer zukünftigen Version nicht mehr unterstützt. Geräte, die Knox Platform for Enterprise unterstützen, können über die Android Enterprise-Aktivierungsarten aktiviert werden. Weitere Informationen finden Sie in Artikel 54614 unter <https://support.blackberry.com/community>.

Aktivierungsart	Beschreibung
Nur geschäftlicher Bereich (vollständig verwaltetes Android Enterprise-Gerät)	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Bei dieser Aktivierungsart muss der Benutzer das Gerät vor der Aktivierung auf die Werkseinstellungen zurücksetzen. Es wird ein geschäftliches Profil und kein persönliches Profil installiert. Der Benutzer muss ein Kennwort für den Zugriff auf das Gerät erstellen. Alle Daten auf dem Gerät werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise ein Kennwort, geschützt.</p> <p>Während der Aktivierung installiert das Gerät BlackBerry UEM Client automatisch und gewährt Administratorberechtigungen. Benutzer können die Administratorberechtigungen nicht aufheben oder die App deinstallieren.</p> <p>Nach der Aktivierung verfügen Nur geschäftlicher Bereich-Geräte nur über einen begrenzten Satz vorinstallierter Standard-Apps, wie Kamera, Telefon und Einstellungen, sowie die Apps, deren Verfügbarkeit Sie als „Erforderlich“ festgelegt haben. Die Liste der beibehaltenen vorinstallierten Apps hängt vom Gerätehersteller und der Betriebssystemversion ab.</p> <p>Für diese Aktivierungsart muss das Gerät vor der Aktivierung auf die Werkseinstellungen zurückgesetzt werden. Wenn BlackBerry UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt.</p>

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – vollständige Kontrolle (vollständig verwaltetes Android Enterprise-Gerät mit geschäftlichem Profil)	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und IT-Richtlinienregeln. Diese Aktivierungsart erstellt ein geschäftliches Profil auf dem Gerät, durch das geschäftliche und persönliche Daten voneinander getrennt werden. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstützt die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in BlackBerry UEM-Protokolldateien.</p> <p>Nach der Aktivierung verfügen Geschäftlich und persönlich – vollständige Kontrolle-Geräte nur über einen begrenzten Satz vorinstallierter Standard-Apps, wie Kamera, Telefon und Einstellungen, im persönlichen Bereich.</p> <p>Für diese Aktivierungsart muss das Gerät vor der Aktivierung auf die Werkseinstellungen zurückgesetzt werden. Wenn BlackBerry UEM Client gelöscht wird oder das geschäftliche Profil vom Gerät entfernt wird, wird es automatisch auf die Werkseinstellungen zurückgesetzt.</p> <p>Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.</p>
Geschäftlich und persönlich – Benutzer-Datenschutz (Android Enterprise mit geschäftlichem Profil)	<p>Diese Aktivierungsart bietet Datenschutz für persönliche Daten, ermöglicht Ihnen jedoch die Verwaltung geschäftlicher Daten mit Befehlen und IT-Richtlinienregeln. Diese Aktivierungsart erstellt ein geschäftliches Profil auf dem Gerät, durch das geschäftliche und persönliche Daten voneinander getrennt werden. Sowohl geschäftliche als auch persönliche Daten werden über Verschlüsselung und Kennwortauthentifizierung geschützt.</p> <p>Die Benutzer müssen dem BlackBerry UEM Client keine Administratorberechtigungen erteilen.</p>
Nur geschäftlicher Bereich - (Samsung Knox)	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und über Samsung Knox-IT-Richtlinienregeln. Diese Aktivierungsart entfernt den persönlichen Bereich und installiert einen geschäftlichen Bereich. Der Benutzer muss ein Kennwort für den Zugriff auf das Gerät erstellen. Alle Daten auf dem Gerät werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstützt die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in BlackBerry UEM-Protokolldateien.</p> <p>Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.</p>

Aktivierungsart	Beschreibung
Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)	<p>Diese Aktivierungsart ermöglicht die Verwaltung des gesamten Geräts über Befehle und die Samsung Knox-IT-Richtlinienregeln. Die Aktivierungsart erstellt einen separaten geschäftlichen Bereich, und der Benutzer muss ein Kennwort einrichten, um auf diesen zuzugreifen. Daten im geschäftlichen Bereich werden durch Verschlüsselung und eine Methode zur Authentifizierung, beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt. Diese Aktivierungsart unterstützt die Protokollierung der Geräteaktivität (SMS, MMS und Telefonanrufe) in BlackBerry UEM-Protokolldateien.</p> <p>Während der Aktivierung müssen Benutzer dem BlackBerry UEM Client Administratorberechtigungen erteilen.</p>

## iOS-Geräte

Aktivierungsart	Beschreibung
MDM-Steuerelemente	<p>Diese Aktivierungsart stellt eine grundlegende Geräteverwaltung über die von iOS zur Verfügung gestellten Gerätesteuerelemente bereit. Es wird kein separater geschäftlicher Bereich auf dem Gerät installiert, und es gibt keine zusätzliche Sicherheit für geschäftliche Daten. Sie können das Gerät mithilfe von Befehlen und IT-Richtlinien steuern.</p>

## Vorbereiten von Benutzern auf die Aktivierung von Geräten

Zur Vorbereitung der Aktivierung von Geräten durch Benutzer sollten Sie ein Aktivierungsprofil erstellen, die Vorlage für die Aktivierungs-E-Mail ändern und ein Aktivierungskennwort für den Benutzer festlegen.

Ein Aktivierungsprofil gibt an, wie viele Geräte und welche Gerätetypen ein Benutzer aktivieren kann, und welche Aktivierungsart für den jeweiligen Gerätetyp verwendet werden soll. Das zugewiesene Aktivierungsprofil gilt nur für Geräte, die der Benutzer aktiviert, nachdem Sie ihm das Profil zugewiesen haben. Geräte, die bereits aktiviert sind, werden nicht automatisch aktualisiert, um dem neuen oder aktualisierten Aktivierungsprofil zu entsprechen.

Wenn Sie in BlackBerry UEM einen Benutzer hinzufügen, wird dem Benutzerkonto das Standard-Aktivierungsprofil zugewiesen. Das standardmäßige Aktivierungsprofil enthält Aktivierungsoptionen, die in einer Dark-Site-Umgebung nicht unterstützt werden. Sie können das Standard-Aktivierungsprofil den Anforderungen entsprechend ändern, oder Sie können ein benutzerdefiniertes Aktivierungsprofil erstellen und dieses Benutzern oder Benutzergruppen zuweisen.

Die Vorlage für die Aktivierungs-E-Mail definiert die E-Mail-Nachricht, die an Benutzer gesendet wird, um ihnen Anweisungen für die Aktivierung ihres Geräts bereitzustellen.

Nach Vervollständigung des Aktivierungsprofils und der E-Mail-Vorlage können Sie ein Aktivierungskennwort für den Benutzer festlegen und eine Aktivierungs-E-Mail senden, damit die Aktivierung abgeschlossen werden kann.

### Erstellen eines Aktivierungsprofils

**Hinweis:** Das Aktivierungsprofil zeigt Optionen für Geräte- und Aktivierungstypen an, die in einer Dark-Site-Umgebung nicht unterstützt werden. Achten Sie beim Erstellen oder Aktualisieren eines Aktivierungsprofils darauf, nur unterstützte Optionen auszuwählen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Richtlinie > Aktivierung**.

3. Klicken Sie auf **+**.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie im Feld **Anzahl der Geräte, die ein Benutzer aktivieren kann** die maximale Anzahl von Geräten ein, die der Benutzer aktivieren kann.
6. Führen Sie in der Dropdown-Liste **Geräteigentümer** eine der folgenden Aktionen aus:
  - Wenn einige Benutzer persönliche Geräte und einige Benutzer geschäftliche Geräte aktivieren, wählen Sie **Nicht angegeben** aus.
  - Wählen Sie **Geschäftlich** aus, wenn die meisten Benutzer geschäftliche Geräte aktivieren.
  - Wählen Sie **Persönlich** aus, wenn die meisten Benutzer ihre persönlichen Geräte aktivieren.
7. Wählen Sie optional einen Organisationshinweis in der Dropdown-Liste **Organisationshinweis zuweisen** aus. Wenn Sie einen Organisationshinweis zuordnen, müssen Benutzer, die BlackBerry 10- oder iOS-Geräte aktivieren, die Mitteilung akzeptieren, um den Aktivierungsvorgang abzuschließen.
8. Aktivieren Sie im Abschnitt **Gerätetypen, die Benutzer aktivieren können** nach Bedarf die Gerätetypen. Gerätetypen, die Sie nicht auswählen, werden im Aktivierungsprofil nicht berücksichtigt, und Benutzer können diese Geräte nicht aktivieren.
9. Führen Sie die folgenden Aktionen für jeden Gerätetyp durch, der im Aktivierungsprofil enthalten ist:
  - a) Klicken Sie auf die Registerkarte für den Gerätetyp.
  - b) Wählen Sie in der Dropdown-Liste **Gerätmodell-Einschränkungen** eine der folgenden Optionen aus:
    - **Keine Einschränkungen:** Benutzer können jedes Gerätmodell aktivieren.
    - **Ausgewählte Gerätmodelle zulassen:** Benutzer können nur die von Ihnen angegebenen Gerätmodelle aktivieren. Verwenden Sie diese Option, um die zulässigen Geräte nur auf einige Modelle zu beschränken.
    - **Ausgewählte Gerätmodelle nicht zulassen:** Benutzer können die von Ihnen angegebenen Gerätmodelle nicht aktivieren. Verwenden Sie diese Option, um die Aktivierung einiger Gerätmodelle oder Geräte bestimmter Hersteller zu blockieren.

Wenn Sie die Gerätmodelle einschränken, die Benutzer aktivieren können, klicken Sie auf **Bearbeiten**, um die Geräte auszuwählen, die Sie zulassen oder einschränken möchten, und klicken Sie dann auf **Speichern**.
  - c) Wählen Sie in der Dropdown-Liste **Zugelassene Mindestversion** die OS-Version aus, die als Mindestanforderung zugelassen ist.
 

Viele ältere OS-Versionen werden von BlackBerry UEM nicht mehr unterstützt. Sie müssen nur dann eine mindestens erforderliche Version auswählen, wenn Sie die früheste Version, die derzeit von BlackBerry UEM unterstützt wird, nicht zulassen möchten. Weitere Informationen zu den unterstützten Versionen [finden Sie in der Kompatibilitätsmatrix](#).
  - d) Wählen Sie die unterstützten Aktivierungstypen aus.
 

Für Samsung Knox-Geräte können Sie mehrere Aktivierungsarten auswählen und sie nach Rangordnung einstufen. Für alle anderen Gerätetypen können Sie nur eine Aktivierungsart auswählen.
10. Wenn Sie bei iOS-Geräten nur beaufsichtigte Geräte aktivieren möchten, wählen Sie **Aktivierung von Geräten ohne Aufsicht nicht zulassen** aus.
11. Führen Sie für Samsung-Geräte die folgenden Aktionen durch:
  - a) Wenn Sie mehr als eine Aktivierungsart ausgewählt haben, klicken Sie auf den Abwärts- bzw. Aufwärtspfeil, um die Rangfolge festzulegen.
  - b) Wenn Sie eine Android Enterprise-Aktivierungsart ausgewählt haben, wählen Sie **Bei der Aktivierung von Android Enterprise-Geräten Premium UEM-Funktionen wie z. B. BlackBerry Secure Connect Plus freischalten**, um die Knox-Plattform für Enterprise-Funktionen zu aktivieren.
  - c) Deaktivieren Sie **Google Play-Konto zum geschäftlichen Bereich hinzufügen**.  
Diese Funktion wird in einer Dark-Site-Umgebung nicht unterstützt.

- d) Wählen Sie im Abschnitt **Optionen für Hardware-Nachweis** die Option **Konformitätsregeln für den Integritätsnachweis während der Aktivierung durchsetzen** aus, wenn BlackBerry UEM bei Aktivierung der Geräte Nachweise senden soll, um sicherzustellen, dass die erforderliche Sicherheits-Patch-Stufe installiert ist.

**12.** Klicken Sie auf **Hinzufügen**.

### **Erstellen einer Vorlage für die Aktivierungs-E-Mail**

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen**.
  2. Klicken Sie auf **E-Mail-Vorlagen**.
  3. Klicken Sie auf **+**. Wählen Sie **Geräteaktivierung** aus.
  4. Geben Sie im Feld **Name** einen Namen für die Vorlage ein.
  5. Bearbeiten Sie den Text im Feld **Betreff** zum Anpassen der Betreffzeile der ersten Aktivierungs-E-Mail.
  6. Geben Sie den Nachrichtentext der Aktivierungs-E-Mail in das Feld **Nachricht** ein.
    - Wählen Sie mithilfe des HTML-Editors die Schriftart aus, und fügen Sie Bilder ein (z. B. das Unternehmenslogo).
    - Fügen Sie Variablen zum Personalisieren des Nachrichtentexts ein (z. B. die Variable %UserDisplayName % zum Einfügen des Empfängernamens). Eine Liste der verfügbaren Variablen finden Sie in [der BlackBerry UEM-Dokumentation für Administratoren](#).
    - Schließen Sie bei BlackBerry 10- und Samsung Knox-Geräten die BlackBerry UEM-Serveradresse ein, die Benutzer für die Aktivierung des Geräts benötigen.
      - Bei BlackBerry 10-Geräten lautet die URL: `http://server.name:8882/SRP_ID/mdm`
      - Bei Samsung Knox-Geräten lautet die URL: `http://server.name:8882/SRP_ID`
    - Klicken Sie zum Anzeigen des Textbeispiels auf **Textvorschlag**.
  7. Wählen Sie **Zwei Aktivierungs-E-Mails senden – die erste mit allen Anweisungen, die zweite mit dem Kennwort** aus, damit Sie das Aktivierungskennwort getrennt von den Aktivierungsanweisungen senden können. Wenn Sie entscheiden, nur eine Aktivierungs-E-Mail-Nachricht zu senden, nehmen Sie unbedingt das Aktivierungskennwort oder die Variable für das Aktivierungskennwort in diese auf.
  8. Geben Sie im Feld **Betreff** eine Betreffzeile für die zweite Aktivierungs-E-Mail ein.
  9. Passen Sie den Nachrichtentext der zweiten Aktivierungs-E-Mail an, die Sie an Benutzer senden. Denken Sie daran, das Aktivierungskennwort oder eine Variable für das Aktivierungskennwort aufzunehmen.
- 10.** Klicken Sie auf **Speichern**.

### **Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail-Nachricht**

Sie können ein Aktivierungskennwort einrichten und einem Benutzer eine Aktivierungs-E-Mail mit den erforderlichen Informationen für die Aktivierung von Geräten senden.

Die E-Mail wird von der E-Mail-Adresse gesendet, die Sie in den SMTP-Servereinstellungen konfiguriert haben.

**Bevor Sie beginnen:** [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).

1. Klicken Sie in der Menüleiste auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach einem Benutzerkonto.
3. Klicken Sie in den Suchergebnissen auf den Namen des Benutzerkontos.
4. Klicken Sie im Bereich „Aktivierungsdetails“ auf **Aktivierungskennwort festlegen**.
5. Wählen Sie in der Dropdown-Liste **AktivierungsoptionStandardmäßige Geräteaktivierung** aus.
6. Führen Sie in der Dropdown-Liste **Aktivierungskennwort** eine der folgenden Aufgaben aus:

- Wenn Sie automatisch ein Kennwort erstellen möchten, wählen Sie **Automatisch ein Geräteaktivierungskennwort generieren und eine E-Mail mit Aktivierungsanweisungen senden**. Wenn Sie diese Option auswählen, müssen Sie eine E-Mail-Vorlage auswählen, mit der die Informationen an den Benutzer gesendet werden sollen.
  - Wenn Sie ein Aktivierungskennwort für den Benutzer festlegen und ggf. eine Aktivierungs-E-Mail senden möchten, wählen Sie **Geräteaktivierungskennwort festlegen** aus.
7. Sie haben optional die Möglichkeit, den Ablauf des Aktivierungszeitraums zu ändern. Der Ablauf des Aktivierungszeitraums legt fest, wie lange das Aktivierungskennwort gültig bleibt.
  8. Wenn Sie möchten, dass das Aktivierungskennwort nur für eine Geräteaktivierung gültig ist, wählen Sie **Aktivierungszeitraum endet nach der Aktivierung des ersten Geräts** aus.
  9. Wählen Sie in der Dropdown-Liste **Vorlage für Aktivierungs-E-Mail** die E-Mail-Vorlage aus, die Sie kopieren möchten.
  10. Klicken Sie auf **Submit**.

### Aktivieren von BlackBerry 10-Geräten

Sie können zulassen, dass Benutzer BlackBerry 10-Geräte über das geschäftliche Wi-Fi-Netzwerk aktivieren, oder Sie können mehrere BlackBerry 10-Geräte für Benutzer mithilfe des BlackBerry Wired Activation Tool aktivieren.

#### Aktivieren von BlackBerry 10-Geräten über das geschäftliche WLAN-Netzwerk

Sie können zulassen, dass Benutzer BlackBerry 10-Geräte über Ihr geschäftliches Wi-Fi-Netzwerk aktivieren. Zum Aktivieren von Geräten benötigen Benutzer die folgenden Informationen:

- Geschäftliche E-Mail-Adresse
- Aktivierungskennwort
- BlackBerry UEM-Serveradresse ([http://server.name:8882/SRP\\_ID/mdm](http://server.name:8882/SRP_ID/mdm))

Sie können die Informationen in der Aktivierungs-E-Mail bereitstellen, die BlackBerry UEM an Benutzer sendet. Siehe [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).

#### Aktivieren eines BlackBerry 10-Geräts

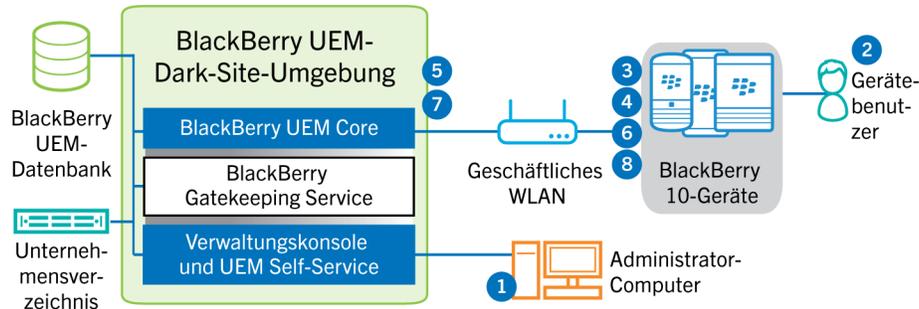
Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Navigieren Sie auf dem Gerät zu **Einstellungen**.
2. Tippen Sie auf **Konten**.
3. Wenn Sie auf diesem Gerät über vorhandene Konten verfügen, tippen Sie auf **Konto hinzufügen**. Andernfalls fahren Sie mit Schritt 4 fort.
4. Tippen Sie auf **E-Mail, Kalender und Kontakte**.
5. Geben Sie Ihre geschäftliche E-Mail-Adresse ein, und tippen Sie auf **Weiter**.
6. Geben Sie im Feld **Kennwort** das empfangene Aktivierungskennwort ein. Tippen Sie auf **Weiter**.  
Sie erhalten eine Warnmeldung, dass Ihr Gerät die Verbindungsinformationen nicht abrufen konnte.
7. Tippen Sie auf **Erweitert**.
8. Tippen Sie auf **Geschäftliches Konto**.
9. Geben Sie im Feld **Serveradresse** die Adresse des Servers ein. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail, die Ihnen zugesendet wurde, oder im BlackBerry UEM Self-Service.
10. Tippen Sie auf **Fertig**.
11. Folgen Sie den Anweisungen auf dem Bildschirm, um den Aktivierungsprozess abzuschließen.

**Wenn Sie fertig sind:** Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Navigieren Sie auf dem Gerät zum BlackBerry Hub, und bestätigen Sie, dass die E-Mail-Adresse vorhanden ist. Navigieren Sie zum Kalender, und bestätigen Sie, dass Kalendertermine vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

### Datenfluss: Aktivieren eines BlackBerry 10-Geräts



#### 1. Führen Sie die folgenden Schritte aus:

- Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
- Weisen Sie dem Benutzer ein Aktivierungsprofil zu.
- Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
  - Automatisches Generieren eines Geräteaktivierungskennworts und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer
  - Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzername und Kennwort direkt oder per E-Mail
  - Weiterleiten der BlackBerry UEM Self-Service-Adresse an den Benutzer, damit dieser ein eigenes Aktivierungskennwort festlegen kann

#### 2. Der Benutzer führt die folgenden Aktionen aus:

- Herstellen der Verbindung zu Ihrem geschäftlichen Wi-Fi-Netzwerk
- Eingeben des Benutzernamens und des Aktivierungskennworts auf dem Gerät
- Im Fall einer Aktivierung vom Typ „Geschäftlich und persönlich – Reguliert“ oder „Nur geschäftlicher Bereich“ akzeptiert er die Geschäftsbedingungen des Unternehmens, denen der Benutzer zustimmen muss

#### 3. Wenn es sich um eine Aktivierung vom Typ „Nur geschäftlicher Bereich“ handelt, werden auf dem Gerät alle bestehenden Daten gelöscht, und das Gerät wird neu gestartet.

#### 4. Das Gerät führt die folgenden Aktionen aus:

- Stellt eine Verbindung mit BlackBerry UEM her.
- Generiert einen gemeinsam genutzten symmetrischen Schlüssel, um die CSR-Datei und die Antwort an BlackBerry UEM mithilfe des Aktivierungskennworts und EC-SPEKE zu schützen.
- Erstellt wie folgt eine verschlüsselte CSR und einen HMAC:
  - Generiert ein Schlüsselpaar für das Zertifikat
  - Erstellt eine PKCS#10 CSR, die den öffentlichen Schlüssel des Schlüsselpaars umfasst

- Verschlüsselt die CSR mithilfe des gemeinsamen symmetrischen Schlüssels und AES-256 im CBC-Modus mit PKCS#5-Padding
  - Berechnet den HMAC der verschlüsselten CSR mithilfe von SHA-256 und hängt ihn an die CSR an
- d. Sendet die verschlüsselte CSR und den HMAC an den BlackBerry UEM
5. BlackBerry UEM führt die folgenden Aktionen aus:
- a. Verifiziert den HMAC der verschlüsselten CSR und entschlüsselt die CSR mithilfe des gemeinsamen symmetrischen Schlüssels
  - b. Ruft den Benutzernamen, die ID des geschäftlichen Bereichs sowie den Namen Ihres Unternehmens aus der BlackBerry UEM-Datenbank ab
  - c. Verpackt das Client-Zertifikat mit den empfangenen Informationen und der vom Gerät gesendeten CSR
  - d. Signiert das Client-Zertifikat mit dem Verwaltungsstammzertifikat des Unternehmens
  - e. Verschlüsselt das Client-Zertifikat, das Verwaltungsstammzertifikat des Unternehmens und die BlackBerry UEM-URL mithilfe des gemeinsamen symmetrischen Schlüssels und AES-256 im CBC-Modus mit PKCS#5-Padding
  - f. Berechnet einen HMAC des verschlüsselten Client-Zertifikats, des Verwaltungsstammzertifikats des Unternehmens und der BlackBerry UEM-URL und hängt ihn an die verschlüsselten Daten an
  - g. Sendet die verschlüsselten Daten und den HMAC an das Gerät
6. Das Gerät führt die folgenden Aktionen aus:
- a. Verifiziert den HMAC
  - b. Entschlüsselt die von BlackBerry UEM empfangenen Daten
  - c. Speichert das Client-Zertifikat und das Verwaltungsstammzertifikat des Unternehmens in seinem Schlüsselspeicher
7. BlackBerry UEM führt die folgenden Aktionen aus:
- a. Weist das neue Gerät einer BlackBerry UEM-Instanz in der Domäne zu
  - b. Sendet Konfigurationsinformationen, einschließlich Enterprise-Konnektivitätseinstellungen, an das Gerät
8. Das Gerät sendet eine Bestätigung über TLS an BlackBerry UEM, die angibt, dass es die IT-Richtlinie und die anderen Daten empfangen und angewendet hat und dass es den geschäftlichen Bereich erstellt hat. Der Aktivierungsprozess ist abgeschlossen.

Die im Aktivierungsprozess herangezogenen Protokolle auf Basis elliptischer Kurven verwenden die von NIST empfohlene 521-Bit-Kurve.

### **Aktivieren von BlackBerry 10-Geräten mithilfe des BlackBerry Wired Activation Tool**

Der BlackBerry Wired Activation Tool ermöglicht die gleichzeitige Aktivierung mehrerer BlackBerry 10-Geräte unter Verwendung von USB-Verbindungen anstelle von drahtlosen Verbindungen. Die Verwendung dieser Methode kann aus verschiedenen Gründen erwünscht sein:

- Schnelle und einfache Aktivierung mehrerer Geräte gleichzeitig
- Beschränkung der Durchführung von Aktivierungen auf die Obhut von Administratoren
- Aktivieren von Geräten und Konfigurieren von Sicherheitsfunktionen (beispielsweise Anforderungen für die Inhaltsverschlüsselung und VPN-Profile), bevor die Geräte an Benutzer ausgehändigt bzw. mit dem Netzwerk des Unternehmens verbunden werden

Sie können mit dem BlackBerry Wired Activation Tool keine Profile und Richtlinien zuweisen. Profile und Richtlinien müssen Benutzern in der BlackBerry UEM-Verwaltungskonsole vor dem Zuweisen und Aktivieren von Geräten mit dem BlackBerry Wired Activation Tool zugewiesen werden. Allerdings müssen Sie keine Aktivierungskennwörter zum Zuweisen und Aktivieren von Geräten mit dem BlackBerry Wired Activation Tool festlegen.

Zum Aktivieren von Geräten mit dem BlackBerry Wired Activation Tool muss auf diesen BlackBerry 10 OS Version 10.3 oder höher ausgeführt werden.

Das BlackBerry Wired Activation Tool wird von BlackBerry UEM Cloud nicht unterstützt.

Um den BlackBerry Wired Activation Tool zu erhalten, wenden Sie sich an den für Sie zuständigen Kundensupportmitarbeiter.

### **Konfigurieren Sie das BlackBerry Wired Activation Tool, und melden Sie sich bei einer BlackBerry UEM-Instanz an.**

Bevor Sie Geräte mit dem BlackBerry Wired Activation Tool aktivieren können, müssen Sie für jede BlackBerry UEM-Instanz, auf die Sie zugreifen müssen, eine Konfiguration erstellen. Nachdem Sie eine Konfiguration erstellt haben, müssen Sie zudem ein Administratorkonto verwenden, damit das BlackBerry Wired Activation Tool auf BlackBerry Web Services zugreifen kann.

1. Doppelklicken Sie im BlackBerry Wired Activation Tool-Installationsordner auf die Datei **BWAT.exe**.
2. Geben Sie im Bildschirm **BES12-Server hinzufügen** im Feld **Name** einen Namen für die Konfiguration ein, die Sie erstellen. Wenn Sie z. B. zwei BlackBerry UEM-Instanzen haben, erstellen Sie für jede eine Konfiguration, und nennen Sie diese „Server 1“ und „Server 2“.
3. Geben Sie im Feld **BlackBerry Web Services-URL** die Webadresse der BlackBerry Web Services-Komponente ein. Die Standardadresse lautet `https://<BlackBerry UEM-Webadresse>:18084`.

Sie können den Port durch Ändern der Einstellung `tomcat.bws.port` in der BlackBerry UEM-Datenbank wechseln.

4. Geben Sie im Feld **BCP-Endpunkt-URL** die Adresse für Geräteaktivierungen ein. Diese wird auch als „Aktivierungs-URL“ bzw. „Servername“ bezeichnet. Die Standardadresse lautet: `http://server.name:8882/SRP_ID/mdm`.

Wenn Sie die Adresse ermitteln möchten, vergewissern Sie sich, dass die Variable `%ActivationURL%` in der Vorlage für die Aktivierungs-E-Mail vorhanden ist, und klicken Sie auf einer beliebigen Benutzerübersichtsseite auf **Aktivierungs-E-Mail anzeigen**.

Falls erforderlich, können Sie auch die Hostadresse und den Port in der BlackBerry UEM-Datenbank nachschlagen. Suchen Sie in der Tabelle `def_cfg_setting_dfn` die Werte `id_setting_definition` für `bdmi.enroll.bcp.host` und `bdmi.enroll.bcp.port`. Verwenden Sie dann die `id_setting_definition`-Werte zum Ermitteln der Werte dieser Einstellungen in `obj_global_cfg_setting`.

5. Klicken Sie auf **Submit**.
6. Wählen Sie im Bildschirm **Anmelden** eine BlackBerry UEM-Konfiguration aus der Dropdown-Liste aus.
7. Geben Sie im Feld **Benutzername** den Benutzernamen eines BlackBerry UEM-Benutzerkontos mit Administratorrechten ein.
8. Geben Sie im Feld **Kennwort** das Kennwort für das Konto ein.
9. Wählen Sie in der Dropdown-Liste **Verzeichnis** eine Authentifizierungsmethode aus.
10. Geben Sie, falls erforderlich, im Feld **Domäne** die Microsoft Active Directory-Domäne an.
11. Klicken Sie auf **Anmelden**.

### **Aktivieren von BlackBerry 10-Geräten mit dem BlackBerry Wired Activation Tool**

#### **Bevor Sie beginnen:**

- Konfigurieren Sie das BlackBerry Wired Activation Tool, und melden Sie sich bei einer BlackBerry UEM-Instanz an.
- Schalten Sie alle verbundenen Geräte ein, und vergewissern Sie sich, dass bei allen Geräten die Ersteinrichtung abgeschlossen ist oder noch nicht begonnen wurde. Sie können keine Geräte aktivieren, wenn die Ersteinrichtung im Gang ist.

1. Verbinden Sie ein oder mehrere BlackBerry 10-Geräte über USB-Kabel mit Ihrem Computer.
2. Überprüfen Sie die Spalte **Status** für jedes Gerät. Führen Sie eine der folgenden Aktionen aus:
  - Wenn in der Spalte „Status“ **Kennwort erforderlich** angezeigt wird, klicken Sie auf **Kennwort erforderlich**, um das Kennwort für das Gerät einzugeben.
  - Wenn in der Spalte „Status“ **Nicht unterstütztes Gerät** angezeigt wird, aktualisieren Sie die Gerätesoftware auf BlackBerry 10 OS Version 10.3 oder höher.
  - Wenn in der Spalte „Status“ **Bereit** angezeigt wird, weisen Sie das Gerät einem Benutzer zu.
3. Suchen Sie mithilfe des Felds **Suchen** das Benutzerkonto, dem Sie das Gerät zuweisen möchten.
4. Klicken Sie im Suchergebnis auf das Benutzerkonto.
5. Klicken Sie im Hauptbereich des Bildschirms auf den Namen eines Benutzerkontos, und ziehen Sie den Namen auf ein Gerät, um dieses dem Benutzer zuzuweisen. Wiederholen Sie diesen Schritt, um weitere Geräte Benutzern zuzuweisen.
6. Aktivieren Sie die Kontrollkästchen neben den Benutzer-/Gerätepaaren, die Sie aktivieren möchten.
7. Klicken Sie auf **Geräte aktivieren**.

Das BlackBerry Wired Activation Tool aktiviert alle ausgewählten Geräte. Prüfen Sie die Spalte „Status“ auf Fortschritt und Ergebnis für die einzelnen Geräte. Wird eine Aktivierung nicht durchgeführt, klicken Sie auf die Meldung in der Spalte „Status“, um weitere Informationen zu Fehlern aufzurufen.

### Aktivieren von Samsung Knox-Geräten

Benutzer können Samsung Knox-Geräte über Ihr geschäftliches Wi-Fi-Netzwerk aktivieren. BlackBerry UEM für Dark Sites bietet keine Unterstützung für die Aktivierungsarten „Samsung Knox MDM“ oder „Geschäftlich und persönlich – Benutzer-Datenschutz - (Samsung Knox)“. BlackBerry UEM für Dark Sites bietet auch keine Unterstützung für Samsung Knox Mobile Enrollment.

**Hinweis:** Samsung Knox-Aktivierungsarten werden in einer zukünftigen Version nicht mehr unterstützt. Geräte, die Knox Platform for Enterprise unterstützen, können über die Android Enterprise-Aktivierungsarten aktiviert werden. Weitere Informationen finden Sie in Artikel 54614 unter <https://support.blackberry.com/community>.

Zum Aktivieren eines Geräts benötigen Benutzer die folgenden Informationen:

- Geschäftliche E-Mail-Adresse
- Aktivierungskennwort
- BlackBerry UEM-Serveradresse ([http://server.name:8882/SRP\\_ID](http://server.name:8882/SRP_ID))

Sie können die Informationen in der Aktivierungs-E-Mail bereitstellen, die BlackBerry UEM an Benutzer sendet. Siehe [Erstellen einer Vorlage für die Aktivierungs-E-Mail](#).

Wenn Ihr Unternehmen Samsung Knox-Geräte in einer Dark-Site-Umgebung verwendet, wurde ein Samsung KLM-Server mit BlackBerry UEM installiert. Samsung Knox-Geräte kommunizieren mit dem KLM-Server über das geschäftliche Wi-Fi-Netzwerk. Wenn Sie Geräte mit Android Enterprise-Aktivierungsarten aktivieren und das KLM-Serverzertifikat von einer internen Zertifizierungsstelle signiert ist, müssen Sie das KLM-Serverzertifikat an Geräte senden, die ein Profil für Zertifizierungsstellenzertifikate verwenden. Weitere Informationen finden Sie in der [Dokumentation für Administratoren von BlackBerry UEM](#).

### Schritte zur Aktivierung von Samsung Knox-Geräten

Schritt	Aktion
<b>1</b>	Erstellen und Zuweisen aller erforderlichen Profile, Apps und IT-Richtlinien für Benutzer. Wenn Sie ein VPN für Samsung Knox-Geräte einrichten möchten, <a href="#">Einrichten des VPNs mit Knox StrongSwan</a> .

Schritt	Aktion
2	Erstellen Sie ein Aktivierungsprofil, und weisen Sie es einem Benutzerkonto oder einer Benutzergruppe zu.
3	Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail-Nachricht.
4	Bereitstellen von Aktivierungsanweisungen für Benutzer von <a href="#">Android Enterprise-Geräten</a> oder <a href="#">Samsung Knox Workspace-Geräten</a> .

### Installieren des BlackBerry UEM Client auf Samsung Knox-Geräten

Benutzer müssen den BlackBerry UEM Client installieren, um ein Samsung Knox-Gerät zu aktivieren. Sie können den UEM Client manuell von BlackBerry herunterladen und an einem Netzwerkspeicherort ablegen, auf den Geräte Zugriff haben. Um die APK-Datei der neuesten UEM Client-App herunterzuladen, besuchen Sie [support.blackberry.com/community](http://support.blackberry.com/community), und lesen Sie Artikel 42607.

Wenn Benutzer Geräte mit der Samsung Knox Workspace- oder Android Enterprise-Aktivierungsart (Geschäftlich und persönlich – Benutzer-Datenschutz) aktivieren, können Sie Benutzer anweisen, den UEM Client abzurufen und zu installieren, bevor sie den Aktivierungsprozess starten.

Bei Geräten, die mit den Aktivierungsarten Android Enterprise (Nur geschäftlicher Bereich) oder (Geschäftlich und persönlich – vollständige Kontrolle) aktiviert werden sollen, muss das Gerät vor dem Start der Aktivierung auf die Werkseinstellungen zurückgesetzt werden. Sie können die Aktivierungsoptionen so festlegen, dass der UEM Client während der Aktivierung von einem Server in Ihrem Netzwerk installiert wird. Um den Download-Speicherort auf dem Gerät anzugeben, können Sie den Speicherort in einem QR Code angeben, den der Benutzer scannt, um die Aktivierung zu starten.

### Festlegen von Aktivierungsoptionen für Android Enterprise-Aktivierungen

Bei Geräten, die mit den Aktivierungsarten Android Enterprise (Nur geschäftlicher Bereich) oder (Geschäftlich und persönlich – vollständige Kontrolle) aktiviert werden sollen, muss das Gerät vor dem Start der Aktivierung auf die Werkseinstellungen zurückgesetzt werden. Sie können die Aktivierungsoptionen so festlegen, dass der BlackBerry UEM Client während der Aktivierung von einem Server in Ihrem Netzwerk installiert wird. Um den Download-Speicherort auf dem Gerät anzugeben, können Sie den Speicherort in einem QR Code angeben, den der Benutzer scannt, um die Aktivierung zu starten.

Sie müssen außerdem eine PAC-Datei erstellen, die verhindert, dass Geräte während der Aktivierung eine Verbindung zu Google Play herzustellen versuchen, und die PAC-Datei am gleichen Speicherort wie die UEM Client APK-Datei speichern.

**Bevor Sie beginnen:** Laden Sie den UEM Client von BlackBerry herunter, und speichern Sie ihn an einem Netzwerkspeicherort, auf den Geräte Zugriff haben. Weitere Informationen finden Sie unter [support.blackberry.com/community](http://support.blackberry.com/community) im Artikel 42607.

1. Erstellen Sie eine PAC-Datei im folgenden Format, in dem die HTTP-URL angegeben ist, unter der die PAC-Datei gehostet wird, und speichern Sie sie an demselben Speicherort wie die UEM Client APK-Datei.

```
function FindProxyForURL(url, host)
{
return "DIRECT";
}
```

Benutzer müssen die **PAC-Webadresse** angeben, wenn sie während der Aktivierung die Wi-Fi-Verbindung auf ihrem Gerät einrichten. Die PAC-Datei muss über den Standard-HTTP-Port 80 verfügbar sein.

2. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen**.
3. Klicken Sie auf **Standards der Aktivierung**.
4. Legen Sie unter **Geräteaktivierungsstandards** die folgenden QR Code-Optionen fest.
  - a) Wählen Sie **QR-Code für Geräteaktivierung zulassen** aus.
  - b) Wählen Sie **Zulassen, dass der QR-Code den Speicherort der Quelldatei der UEM Client-App enthält**.
  - c) Geben Sie im Feld **Speicherort der Quelldatei für die UEM Client-App** den Netzwerkspeicherort an, an dem die APK-Datei gespeichert ist.
5. Stellen Sie sicher, dass die folgenden Optionen nicht ausgewählt sind:
  - **Aktivierungsart MDM-Steuerelemente für Android-Geräte aktivieren**
  - **QR-Codes für das Entsperren von BlackBerry Dynamics-Apps verwenden**
  - **Registrierung mit BlackBerry Infrastructure einschalten**
6. Klicken Sie auf **Speichern**.

### **Aktivieren eines Android Enterprise-Geräts**

Diese Anweisungen gelten für die Aktivierungsarten Android Enterprise (Nur geschäftlicher Bereich) oder (Geschäftlich und persönlich – vollständige Kontrolle). Für diese Geräte muss das Gerät auf die Werkseinstellungen zurückgesetzt werden, bevor die Aktivierung gestartet werden kann.

Für Aktivierungen von Android Enterprise (Geschäftlich und persönlich – Benutzer-Datenschutz) befolgen Sie die Anweisungen zum [Aktivieren eines Samsung Knox Workspace-Geräts](#).

Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Wenn Ihnen auf dem zu aktivierenden Gerät der Willkommen-Bildschirm der Geräteeinrichtung nicht angezeigt wird, setzen Sie das Gerät auf die werksseitigen Standardeinstellungen zurück.
2. Tippen Sie siebenmal auf den Gerätebildschirm.  
Auf dem Gerät wird ein QR-Code-Leser geöffnet.
3. Scannen Sie den QR-Code, den Sie von Ihrem Administrator erhalten haben.
4. Geben Sie die Informationen an, um eine Verbindung zu Ihrem WLAN-Netzwerk herzustellen, einschließlich der vom Administrator bereitgestellten **PAC-Webadresse**.  
Das Gerät installiert den BlackBerry UEM Client und startet den Aktivierungsvorgang. Der Aktivierungsvorgang dauert einige Minuten.
5. Reagieren Sie auf alle Eingabeaufforderungen auf dem Gerät, einschließlich der Eingabe des Aktivierungskennworts, falls erforderlich, der Annahme von Lizenzvereinbarungen, der Einrichtung eines Arbeitsprofils und der Erstellung eines Gerätekenworts.
6. Schließen Sie das Gerät je nach Serverkonfiguration bei einer Unterbrechung der Aktivierung ggf. über ein USB-C-Kabel an einen Computer im Netzwerk an, bevor Sie fortfahren.

**Wenn Sie fertig sind:** Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie den UEM Client auf dem Gerät. Tippen Sie auf **Info**. Überprüfen Sie im Abschnitt **Aktiviertes Gerät**, dass die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

## Aktivieren eines Samsung Knox Workspace-Geräts

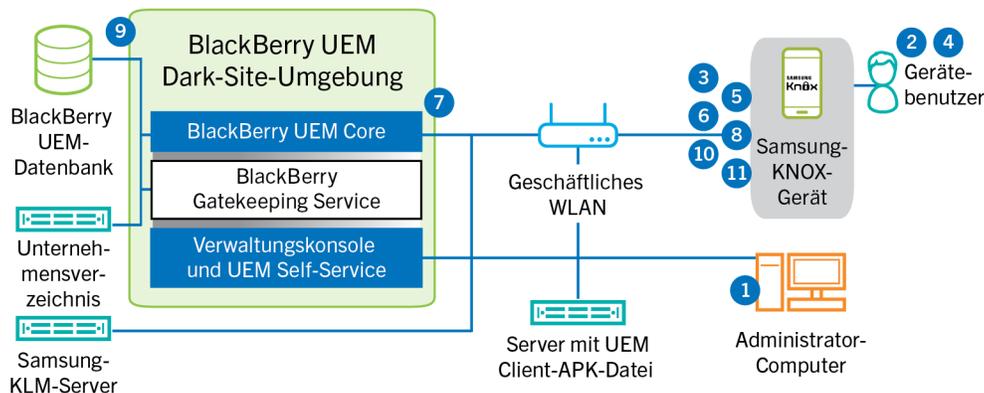
Diese Anweisungen gelten auch für Aktivierungen von Android Enterprise (Geschäftlich und persönlich – Benutzer-Datenschutz). Senden Sie die folgenden Aktivierungsanweisungen an den Gerätebenutzer.

1. Verbinden Sie das Gerät mit dem geschäftlichen Wi-Fi-Netzwerk.
2. Laden Sie den BlackBerry UEM Client von dem Speicherort herunter, den Ihr Administrator angegeben hat, und installieren Sie ihn.
3. Tippen Sie auf dem Gerät auf **UEM Client**.
4. Lesen Sie die Lizenzvereinbarung. Tippen Sie auf **Ich stimme zu**.
5. Geben Sie Ihre geschäftliche E-Mail-Adresse ein. Tippen Sie auf **Weiter**.
6. Geben Sie die Serveradresse ein. Tippen Sie auf **Weiter**. Die Serveradresse finden Sie entweder in der Aktivierungs-E-Mail-Nachricht, die Ihnen zugesendet wurde, oder in BlackBerry UEM Self-Service.
7. Geben Sie Ihr Aktivierungskennwort ein. Tippen Sie auf **Mein Gerät aktivieren**.
8. Tippen Sie auf **Weiter**.
9. Tippen Sie auf **Aktivieren**.

**Wenn Sie fertig sind:** Um zu überprüfen, ob der Aktivierungsprozess erfolgreich abgeschlossen wurde, führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie den UEM Client auf dem Gerät. Tippen Sie auf **Info**. Überprüfen Sie im Abschnitt **Aktiviertes Gerät**, dass die Geräteinformationen und der Aktivierungszeitstempel vorhanden sind.
- Überprüfen Sie im BlackBerry UEM Self-Service, ob Ihr Gerät als aktiviertes Gerät aufgeführt ist. Nachdem Sie das Gerät aktiviert haben, kann es bis zu zwei Minuten dauern, bis der Status aktualisiert wird.

## Datenfluss: Ein Android Enterprise-Gerät aktivieren

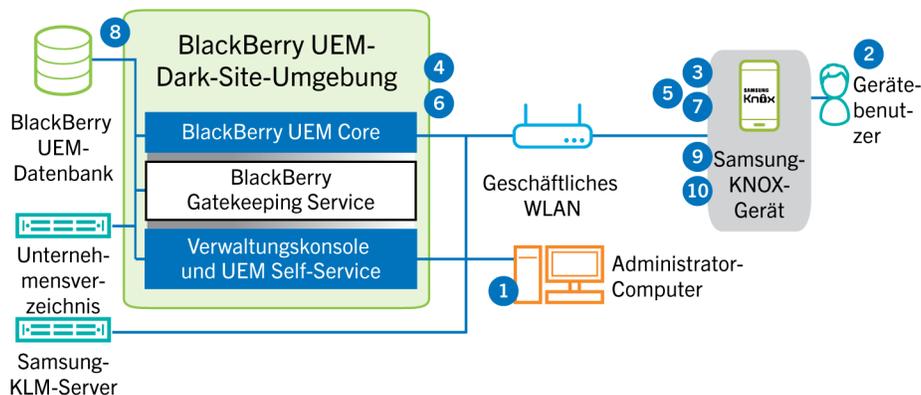


Dieser Datenfluss gilt für Geräte, die mit den Aktivierungsarten Android Enterprise (Nur geschäftlicher Bereich) oder (Geschäftlich und persönlich – vollständige Kontrolle) aktiviert wurden.

1. Führen Sie die folgenden Schritte aus:
  - a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
  - b. Stellen Sie sicher, dass die Aktivierungsart „Android Enterprise (Nur geschäftlicher Bereich)“ oder „Geschäftlich und persönlich – vollständige Kontrolle“ dem Benutzer zugewiesen ist.
  - c. Lassen Sie zu, dass Aktivierungs-QR-Codes das Aktivierungskennwort und den Speicherort zum Herunterladen des BlackBerry UEM Client s enthalten.
2. Der Benutzer setzt sein Gerät auf die werkseitigen Standardeinstellungen zurück.
3. Das Gerät wird neu gestartet und zeigt einen Begrüßungs- oder Startbildschirm an.

4. Der Benutzer führt die folgenden Aktionen aus:
  - a. Öffnet die Aktivierungs-E-Mail, die er auf seinem Computer oder einem anderen Gerät erhalten hat
  - b. Tippt siebenmal auf den Gerätebildschirm, um einen QR-Codeleser zu öffnen
  - c. Verbindet das Gerät mit dem geschäftlichen Wi-Fi-Netzwerk.
  - d. Scannt den QR-Code in der Aktivierungs-E-Mail
5. Das Gerät führt die folgenden Aktionen aus:
  - a. Fordert den Benutzer auf, das Gerät zu entschlüsseln und startet neu
  - b. Lädt den im QR-Code angegebenen UEM Client vom Download-Speicherort herunter und installiert ihn
6. Der UEM Client stellt eine Verbindung mit BlackBerry UEM her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Geräteerkennung.
7. BlackBerry UEM führt folgende Aktionen aus:
  - a. Überprüfen der Anmeldeinformationen auf Gültigkeit
  - b. Erstellen eines Gerätekennworts
  - c. Verknüpfen der Geräteinstanz mit dem angegebenen Benutzerkonto in der BlackBerry UEM-Datenbank
  - d. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
  - e. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät
8. Der UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
9. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet die angeforderten Konfigurationsinformationen an das Gerät.
10. Der UEM Client überprüft, ob das Gerät Knox Platform for Enterprise verwendet und eine unterstützte Version ausführt. Wenn das Gerät Knox Platform for Enterprise verwendet, stellt das Gerät eine Verbindung mit dem lokalen Samsung-KLM-Server her und aktiviert die Knox-Verwaltungslizenz. Nach der Aktivierung wendet UEM Client die entsprechenden IT-Richtlinienregeln für Android Enterprise an.
11. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

#### Datenfluss: Geräte für die Verwendung von Knox Workspace aktivieren



1. Führen Sie die folgenden Schritte aus:
  - a. Fügen Sie BlackBerry UEM einen Benutzer als lokales Benutzerkonto hinzu, oder verwenden Sie die Kontoinformationen aus dem Unternehmensverzeichnis.
  - b. Stellen Sie sicher, dass die Aktivierungsart „Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)“ oder „Nur geschäftlicher Bereich - (Samsung Knox)“ dem Benutzer zugewiesen ist.
  - c. Weisen Sie den Benutzer an, den BlackBerry UEM Client herunterzuladen und zu installieren.

- d. Es gibt folgende Möglichkeiten, Aktivierungsdetails für Benutzer bereitzustellen:
- Automatisches Generieren eines Geräteaktivierungskennworts und Senden einer E-Mail mit Aktivierungsanweisungen für den Benutzer
  - Einrichten eines Geräteaktivierungskennworts und Informieren des Benutzers über Benutzernamen und Kennwort direkt oder per E-Mail
  - Weiterleiten der BlackBerry UEM Self-Service-Adresse an den Benutzer, damit dieser ein eigenes Aktivierungskennwort festlegen kann
2. Der Benutzer führt die folgenden Aktionen aus:
    - Herstellen der Verbindung zu Ihrem geschäftlichen Wi-Fi-Netzwerk
    - Herunterladen und Installieren des UEM Client auf dem Gerät
    - Öffnen des UEM Client und Eingeben der E-Mail-Adresse und des Aktivierungskennworts
  3. Der UEM Client stellt eine Verbindung mit BlackBerry UEM her und sendet eine Aktivierungsanforderung an BlackBerry UEM. Die Aktivierungsanforderung enthält den Benutzernamen, das Kennwort, das Betriebssystem des Geräts und die eindeutige Geräteerkennung.
  4. BlackBerry UEM führt folgende Aktionen aus:
    - a. Überprüfen der Anmeldeinformationen auf Gültigkeit
    - b. Erstellen eines Gerätekennworts
    - c. Verknüpfen der Geräteinstanz mit dem angegebenen Benutzerkonto in der BlackBerry UEM-Datenbank
    - d. Hinzufügen der ID der Anmeldungssitzung zu einer HTTP-Sitzung
    - e. Senden einer erfolgreichen Authentifizierungsnachricht an das Gerät
  5. Der UEM Client erstellt mithilfe der von BlackBerry UEM empfangenen Informationen eine CSR-Datei und sendet eine Anforderung für ein Client-Zertifikat über HTTPS an BlackBerry UEM.
  6. BlackBerry UEM führt die folgenden Aktionen aus:
    - a. Überprüfen der Anforderung des Client-Zertifikats mit der ID der Anmeldungssitzung in der HTTP-Sitzung
    - b. Signieren der Anforderung des Client-Zertifikats mit dem Stammzertifikat
    - c. Senden des signierten Client-Zertifikats und des Stammzertifikats zurück an den UEM Client

Eine gegenseitig authentifizierte TLS-Sitzung wird zwischen dem UEM Client und BlackBerry UEM hergestellt.
  7. Der UEM Client fordert alle Konfigurationsinformationen an und sendet die Geräte- und Softwareinformationen an BlackBerry UEM.
  8. BlackBerry UEM speichert die Geräteinformationen in der Datenbank und sendet die angeforderten Konfigurationsinformationen an das Gerät.
  9. Der UEM Client überprüft, ob das Gerät Knox Workspace verwendet und eine unterstützte Version ausführt. Wenn das Gerät Knox Workspace verwendet, stellt das Gerät eine Verbindung mit dem lokalen Samsung-KLM-Server her und aktiviert die Knox-Verwaltungslizenz. Nach der Aktivierung wendet UEM Client die Knox-MDM- und die Knox Workspace IT-Richtlinienregeln an.
  10. Das Gerät sendet eine Bestätigung an BlackBerry UEM, dass es die Konfigurationsinformationen empfangen und angewendet hat. Der Aktivierungsprozess ist abgeschlossen.

Nachdem die Aktivierung abgeschlossen ist, wird der Benutzer aufgefordert, ein Kennwort für den geschäftlichen Bereich für Knox Workspace zu erstellen. Die Daten im Knox Workspace sind durch Verschlüsselung und eine Authentifizierungsmethode, wie beispielsweise Kennwort, PIN, Muster oder Fingerabdruck, geschützt.

**Hinweis:** Wenn das Gerät mit der Aktivierungsart „Nur geschäftlicher Bereich - (Samsung Knox)“ aktiviert wurde, wird der persönliche Speicherplatz nach der Einrichtung von Knox Workspace entfernt.

## Aktivieren von iOS-Geräten

Wenn Sie zulassen möchten, dass Benutzer iOS-Geräte in einer Dark-Site-Umgebung benutzen können, müssen Sie die Geräte mithilfe von Apple Configurator 2 vorbereiten. BlackBerry UEM bietet keine Unterstützung für

Geräte mit Apple-DEP-Registrierung. Benutzer können die Aktivierung vorbereiteter Geräte ohne Verwendung der BlackBerry UEM Client-App durchführen. Sie brauchen nur ihren Benutzernamen und ihr Aktivierungskennwort.

Wenn die Geräte aktiviert werden, sendet BlackBerry UEM die IT-Richtlinien und Profile, die Sie Benutzern auf den Geräten zugewiesen haben.

### Schritte zur Aktivierung von iOS-Geräten

Schritt	Aktion
1	Hinzufügen von BlackBerry UEM-Serverinformationen zu Apple Configurator 2.
2	Vorbereiten von iOS-Geräten mit Apple Configurator 2.
3	Erstellen Sie ein Aktivierungsprofil, und weisen Sie es einem Benutzerkonto oder einer Benutzergruppe zu.
4	Einrichten eines Aktivierungskennworts und Senden einer Aktivierungs-E-Mail-Nachricht.
5	Verteilen Sie die Geräte an die Benutzer, und fordern Sie sie zum Abschluss der Einrichtung auf.

#### Hinzufügen von BlackBerry UEM-Serverinformationen zu Apple Configurator 2

**Bevor Sie beginnen:** Laden Sie die aktuelle Version des Apple Configurator 2 von Apple herunter, und installieren Sie ihn.

1. Wählen Sie im Apple Configurator 2-Menü **Einstellungen > Server** aus.
2. Klicken Sie auf **+ > Weiter**.
3. Geben Sie im Feld **Name** einen Namen für den Server ein.
4. Geben Sie in das Feld **Hostname oder URL** die BlackBerry UEM Server-URL im folgenden Format ein: *<http oder https>://<Servername>:<Port>*, wobei die Standardportnummer 8885 ist. Weitere Informationen zu Porteinstellungen finden Sie unter [BlackBerry UEM-Abhörports](#) in der Dokumentation zur Planung.
5. Klicken Sie auf **Weiter**.
6. Schließen Sie das **Server**-Fenster.

#### Vorbereiten von iOS-Geräten mit Apple Configurator 2

Wenn Sie ein Gerät vorbereiten, bereinigt Apple Configurator 2 das Gerät und aktualisiert das Betriebssystem auf die neueste Version.

**Bevor Sie beginnen:** [Hinzufügen von BlackBerry UEM-Serverinformationen zu Apple Configurator 2](#).

1. Öffnen Sie Apple Configurator 2.
2. Verbinden Sie ein oder mehrere iOS-Geräte mit Ihrem Computer.
3. Klicken Sie auf **Vorbereiten**.
4. Wählen Sie in der Dropdown-Liste **Konfiguration** die Option **Manuell** aus. Klicken Sie auf **Weiter**.

5. Wählen Sie in der Dropdown-Liste **Server** den BlackBerry UEM-Server aus. Klicken Sie auf **Weiter**.
6. Aktivieren Sie ggf. das Kontrollkästchen **Unter Aufsicht stellen**. Klicken Sie auf **Weiter**.
7. Wenn Sie **Unter Aufsicht stellen** ausgewählt haben, vervollständigen Sie die Unternehmensinformationen.
8. Klicken Sie auf **Vorbereiten**, und warten Sie, während das Gerät vorbereitet wird. Dieser Prozess dauert bis zu 15 Minuten.

**Wenn Sie fertig sind:** Verteilen Sie die Geräte an Benutzer, damit diese die Aktivierung abschließen können.

## Verwalten von BlackBerry 10-Geräten

Details zum Verwalten von BlackBerry 10-Geräten und -Gerätebenutzern finden Sie in der [BlackBerry UEM-Dokumentation für Administratoren](#).

Beachten Sie bei der Verwaltung von BlackBerry 10-Geräten in einer Dark-Site-Umgebung bitte Folgendes.

Überlegungen zu Dark Sites	Beschreibung
Herstellen einer Verbindung mit den Ressourcen Ihres Unternehmens	In einer Dark-Site-Umgebung können BlackBerry 10-Geräte nur über das geschäftliche Wi-Fi-Netzwerk oder ein VPN eine Verbindung mit Ihrem Netzwerk herstellen. Wenn Sie ein VPN verwenden möchten, vergewissern Sie sich, dass eine entsprechende VPN-App auf dem Gerät installiert und ein VPN-Profil eingerichtet wurde.
App-Verwaltung	BlackBerry UEM für Dark Sites unterstützt keine Verbindungen mit BlackBerry World. Sie können keine öffentlichen Apps zur App-Liste von Geräten hinzufügen.

## Verwalten von Samsung Knox-Geräten

Details zum Verwalten von Samsung Knox-Geräten und -Gerätebenutzern [finden in der BlackBerry UEM-Dokumentation für Administratoren](#).

Beachten Sie bei der Verwaltung von Samsung Knox-Geräten in einer Dark-Site-Umgebung bitte Folgendes.

Überlegungen zu Dark Sites	Beschreibung
Herstellen einer Verbindung mit den Ressourcen Ihres Unternehmens	In einer Dark-Site-Umgebung können Samsung Knox-Geräte nach der Aktivierung über ein VPN eine Verbindung mit BlackBerry UEM und Ihren Ressourcen herstellen. Weitere Informationen finden Sie unter „ <a href="#">Einrichten des VPNs mit Knox StrongSwan</a> “.
App-Verwaltung	BlackBerry UEM für Dark Sites unterstützt keine Verbindungen mit Google Play. Sie können keine öffentlichen Apps zur App-Liste von Geräten hinzufügen.
E-Mail- und Terminplannerdaten	Die Standard-E-Mail-App auf Samsung Knox-Geräten muss eine Verbindung mit der Samsung-Infrastruktur herstellen, bevor sie Daten senden und empfangen kann. Sie können auswählen, ob Sie diese Verbindung zulassen oder eine andere E-Mail-App auf Samsung Knox-Geräten verwenden.

Überlegungen zu Dark Sites	Beschreibung
Gerätebenachrichtigungen	Das Senden von Benachrichtigungen an Samsung Knox-Geräte über GCM wird in einer Dark-Site-Umgebung nicht unterstützt. Der BlackBerry UEM Client ruft regelmäßig Updates von BlackBerry UEM ab.

## Einrichten des VPNs mit Knox StrongSwan

Sie können den VPN-Zugriff auf Ihre Umgebung für Samsung Knox-Geräte einrichten.

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

1. Fügen Sie das Knox Service Plugin und die Android VPN Management für Knox StrongSwan-Apps der [App-Liste](#) hinzu.
2. Wählen Sie die Knox Service Plugin-App aus, und klicken Sie auf **+**, um die [Konfigurationsoptionen für die App](#) festzulegen.
  - a) Wählen Sie unter **VPN-Profil** die Option **Integriertes Knox-VPN** aus.
  - b) Legen Sie unter **Parameter für Integriertes Knox-VPN (für StrongSwan)** die folgenden Optionen fest:
    - Legen Sie den **Authentifizierungstyp** auf "ipsec\_ike2\_rsa" fest.
    - Legen Sie den **Alias für das Benutzerzertifikat** als Benutzername mit Anhang „\_1 [Knox]“ fest. Sie können [Variablen](#) für den Benutzernamen verwenden (z. B. %UserFirstName% %UserLastName% \_1 [Knox].)
    - Legen Sie den **Alias für Zertifizierungsstellenzertifikat** als Benutzername mit Anhang „ [Knox]“ fest. Sie können [Variablen](#) für den Benutzernamen verwenden (z. B. %UserFirstName% %UserLastName% [Knox].)
3. Weisen Sie die App dem Benutzer zu.
4. [Erstellen Sie ein Profil für Zertifizierungsstellenzertifikate](#), um das VPN-Serverzertifikat an Geräte zu senden und Benutzern zuzuweisen.
5. [Fügen Sie ein VPN-Clientzertifikat](#) für jeden Benutzer hinzu.

## Verwalten von iOS-Geräten

Details zum Verwalten von iOS-Geräten und -Gerätebenutzern [finden in der BlackBerry UEM-Dokumentation für Administratoren](#).

Beachten Sie bei der Verwaltung von iOS-Geräten in einer Dark-Site-Umgebung bitte Folgendes.

Überlegungen zu Dark Sites	Beschreibung
Herstellen einer Verbindung mit den Ressourcen Ihres Unternehmens	In einer Dark-Site-Umgebung können iOS-Geräte nach der Aktivierung über ein VPN eine Verbindung mit BlackBerry UEM und Ihren Ressourcen herstellen. Wenn Sie ein VPN verwenden möchten, vergewissern Sie sich, dass eine entsprechende VPN-App auf dem Gerät installiert und ein VPN-Profil eingerichtet wurde.
App-Verwaltung	BlackBerry UEM für Dark Sites unterstützt keine Verbindungen mit dem Apple App Store. Sie können keine öffentlichen Apps zur App-Liste von Geräten hinzufügen.

<b>Überlegungen zu Dark Sites</b>	<b>Beschreibung</b>
Konformitätsprofile	Da der BlackBerry UEM Client-Client für iOS-Geräte in einer Dark-Site-Umgebung nicht unterstützt wird, werden auch keine Konformitätsprofile unterstützt.

# Produktdokumentation

Die folgende BlackBerry UEM-Dokumentation enthält nützliche Informationen für die Verwaltung von BlackBerry UEM in einer Dark-Site-Umgebung.

Wenn die Sicherheitsanforderungen für Ihre Dark-Site-Umgebung verhindern, dass Sie von der Verwaltungskonsole auf die BlackBerry UEM-Dokumentation zugreifen, können Sie PDF-Versionen der Dokumentation von einem Standort mit vollständigem Internetzugriff herunterladen oder Ihren Kundensupportmitarbeiter von BlackBerry bitten, Ihnen die Dokumentation zuzusenden.

Ressource	Beschreibung
<b>Versionshinweise</b>	<ul style="list-style-type: none"><li>• Beschreibung behobener Probleme</li><li>• Beschreibung von bekannten Problemen und potenziellen Workarounds</li><li>• Neuerungen</li></ul>
<b>Installation und Upgrade</b>	<ul style="list-style-type: none"><li>• Systemanforderungen</li><li>• Installationsanweisungen</li><li>• Upgrade-Anweisungen</li></ul>
<b>Konfiguration</b>	<ul style="list-style-type: none"><li>• Anweisungen zur Konfiguration von Serverkomponenten vor der Verwaltung von Benutzern und ihren Geräten</li><li>• Anweisungen zur Migration von Daten aus einer bestehenden BlackBerry UEM-Datenbank</li></ul>
<b>Administration</b>	<ul style="list-style-type: none"><li>• Grundlegende und erweiterte Administrationaufgaben für alle unterstützten Gerätetypen</li><li>• Anweisungen zum Erstellen von Benutzerkonten, Gruppen, Rollen und Administratorkonten</li><li>• Anweisungen zur Aktivierung von Geräten</li><li>• Anweisungen zum Erstellen und Zuweisen von IT-Richtlinien und Profilen</li><li>• Anweisungen zum Verwalten von Apps auf Geräten</li><li>• Beschreibungen der Profileinstellungen</li><li>• Beschreibungen der IT-Richtlinienregeln für BlackBerry 10-, iOS- und Android-Geräte</li></ul>
<b>Kompatibilitätsmatrix</b>	<ul style="list-style-type: none"><li>• Liste der unterstützten Betriebssysteme, Datenbankserver und Browser für den BlackBerry UEM-Server</li><li>• Liste der unterstützten Gerätebetriebssysteme</li></ul>

# Rechtliche Hinweise

©2022 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

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, ZUFRIEDENSTELLENDE QUALITÄT ODER DES EIGENTUMSRECHTS ABGELEHNT. DIES GILT AUCH FÜR ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, DIE SICH AUS EINEM GESETZ, EINER GEPFLOGENHEIT, CHANCEN BZW. HANDELSGEPFLOGENHEITEN ERGEBEN ODER IM ZUSAMMENHANG MIT DER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER MANGELNDE LEISTUNG VON SOFTWARE, HARDWARE, DIENSTEN ODER DRITTPRODUKTEN UND -DIENSTEN STEHEN, AUF DIE HIER VERWIESEN WIRD. MÖGLICHERWEISE GELTEN FÜR SIE ZUDEM ANDERE LANDESSPEZIFISCHE RECHTE. IN MANCHEN RECHTSGEBIETEN IST DER AUSSCHLUSS ODER DIE EINSCHRÄNKUNG KONKLUDENTER GEWÄHRLEISTUNGEN UND BEDINGUNGEN NICHT ZULÄSSIG. IN DEM GESETZLICH ZULÄSSIGEN UMFANG WERDEN SÄMTLICHE KONKLUDENTEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN IM ZUSAMMENHANG MIT DER DOKUMENTATION, DIE EINGESCHRÄNKT WERDEN KÖNNEN, 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 JEDLICHER ART, DIE IM ZUSAMMENHANG MIT DIESER DOKUMENTATION ODER IHRER VERWENDUNG, DER LEISTUNG ODER NICHTLEISTUNG JEDLICHER SOFTWARE, HARDWARE, DIENSTE ODER DRITTPRODUKTEN UND -DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD, STEHEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE FOLGENDEN SCHÄDEN: DIREKTE, VERSCHÄRFTE SCHADENERSATZ NACH SICH ZIEHENDE, BEILÄUFIG ENTSTANDENE, INDIREKTE, KONKRETE,

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

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

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

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

Bevor Sie Drittprodukte bzw. -dienste abonnieren, installieren oder verwenden, müssen Sie sicherstellen, dass Ihr Mobilfunkanbieter sich mit der Unterstützung aller zugehörigen Funktionen einverstanden erklärt hat. Einige Mobilfunkanbieter bieten möglicherweise keine Internet-Browsing-Funktion in Zusammenhang mit einem Abonnement für den BlackBerry® Internet Service an. Erkundigen Sie sich bei Ihrem Diensteanbieter 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 GARANTIEEN, 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