BlackBerry UEM

Sichern von Verbindungen mit PKI

Verwenden

12.13

Inhalt

Zertifikate und PKI

Ein PKI-Zertifikat ist ein digitales Dokument, das von einer Zertifizierungsstelle erstellt wurde, die Identität eines Zertifikatempfängers überprüft und diese mit einem öffentlichen Schlüssel verknüpft. Für jedes Zertifikat ist ein entsprechender privater Schlüssel vorhanden, der getrennt gespeichert wird. Der öffentliche Schlüssel und der private Schlüssel bilden ein asymmetrisches Schlüsselpaar, das zur Datenverschlüsselung und zur Identitätsauthentifizierung verwendet werden kann. Eine Zertifizierungsstelle signiert das Zertifikat und bescheinigt, dass Institutionen, die der Zertifizierungsstelle vertrauen, auch dem Zertifikat vertrauen können.

Je nach Gerätefunktionen und Aktivierungsart können Zertifikate von Geräten und Apps für Folgendes verwendet werden:

- Authentifizieren mittels SSL/TLS, wenn eine Verbindung zu Webseiten hergestellt wird, die HTTPS verwenden
- Authentifizieren mit einem geschäftlichen Mailserver
- Authentifizieren mit einem geschäftlichen Wi-Fi-Netzwerk oder einem VPN
- Verschlüsseln und Signieren von E-Mail-Nachrichten mittels S/MIME-Schutz

Mehrfachzertifikate, die für verschiedene Zwecke verwendet werden, können auf einem Gerät gespeichert werden.

Schritte zur Nutzung von Zertifikaten

Wenn Sie PKI-Zertifikate mit Geräten oder Apps verwenden, führen Sie die folgenden Aktionen durch:

Schritt	Aktion
1	Falls erforderlich verbinden Sie BlackBerry UEM mit der PKI-Software Ihres Unternehmens.
2	Erstellen Sie mindestens ein Profil für Zertifizierungsstellenzertifikate, über das Zertifizierungsstellenzertifikate an Geräte und Apps gesendet werden sollen.
3	Erstellen Sie Profile für SCEP, Anmeldeinformationen oder gemeinsam genutzte Zertifikate, oder laden Sie Zertifikate für einen bestimmten Benutzer hoch, um Clientzertifikate an Geräte und Apps zu senden.
4	Verknüpfen Sie die Zertifikatprofile ggf. mit Wi-Fi-, VPN- oder E-Mail-Profilen.
5	Weisen Sie Benutzerkonten, Benutzergruppen oder Gerätegruppen ggf. Zertifikatprofile zu.
6	Wenn Sie Zertifikate mit einer BlackBerry Dynamics-App verwenden, wählen Sie in den App-Einstellungen „ BlackBerry Dynamics-Apps die Verwendung von Benutzerzertifikaten, SCEP-Profilen und Profilen für Benutzeranmeldeinformationen erlauben“ aus.

Vernetzung von BlackBerry UEM und der PKI-Software Ihrer Organisation

Wenn Ihre Organisation eine PKI-Lösung zur Ausgabe von Zertifikaten verwendet, können Sie die zertifikatsbasierte Authentifizierung dieser PKI-Services auf die Geräte erweitern, die Sie mit BlackBerry UEM verwalten.

Entrust-Produkte (z. B. Entrust IdentityGuard und Entrust Authority Administration Services) sowie OpenTrust-Produkte (z. B. OpenTrust PKI und OpenTrust CMS) stellen Zertifizierungsstellen bereit, die Clientzertifikate ausgeben. Sie können eine Verbindung mit der PKI-Software Ihrer Organisation konfigurieren und Profile verwenden, um das Zertifizierungsstellenzertifikat und Clientzertifikate an Geräte zu senden.

Für Geräte mit BlackBerry Dynamics-Aktivierung können Sie ebenfalls eine PKI-Verbindung einrichten, die eine Verbindung zwischen BlackBerry UEM und einem Zertifizierungsstellenserver für die Anmeldung von Zertifikaten für BlackBerry Dynamics-Apps herstellt, oder verwenden Sie eine App, die die zertifikatbasierte Registrierung unterstützt, z. B. Purebred.

Herstellen einer Verbindung zwischen BlackBerry UEM und der Entrust-Software Ihres Unternehmens

Um zu ermöglichen, dass BlackBerry UEM Zertifikate, die von der Entrust-Software Ihres Unternehmens ausgestellt wurden (z. B. Entrust IdentityGuard oder Entrust Authority Administration Services), an Geräte und BlackBerry Dynamics-Apps sendet, können Sie eine Verbindung zur Entrust-Software Ihres Unternehmens zu BlackBerry UEM hinzufügen.

Bevor Sie beginnen: Kontaktieren Sie den Entrust-Administrator Ihres Unternehmens, um Folgendes zu erhalten:

- URL des Entrust MDM Web Service
- Anmeldeinformationen für ein Entrust-Administratorkonto, das zum Herstellen der Verbindung zwischen BlackBerry UEM und der Entrust-Software verwendet werden kann
- Entrust-Zertifizierungsstellenzertifikat, das den öffentlichen Schlüssel (.der, .pem oder .cert) enthält; BlackBerry UEM verwendet dieses Zertifikat zum Aufbau von SSL-Verbindungen zum Entrust-Server

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie auf **Externe Integration > Zertifizierungsstelle**.
3. Klicken Sie auf **Hinzufügen einer Entrust-Verbindung**.
4. Geben Sie im Feld **Verbindungsname** einen Namen für die Verbindung ein.
5. Geben Sie im Feld **URL** die URL für den Entrust MDM Web Service ein.
6. Geben Sie im Feld **Benutzername** den Benutzernamen des Entrust-Administratorkontos ein.
7. Geben Sie im Feld **Kennwort** das Kennwort für das Entrust-Administratorkonto ein.
8. Um ein Zertifizierungsstellenzertifikat hochzuladen, das BlackBerry UEM den Aufbau von SSL-Verbindungen zum Entrust-Server ermöglicht, klicken Sie auf **Durchsuchen**. Navigieren Sie zu dem CA-Zertifikat, und wählen Sie es aus.
9. Um die Verbindung zu testen, klicken Sie auf **Verbindung testen**.
10. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Ein Profil mit Benutzeranmeldeinformationen zum Senden von Zertifikaten von Ihrer PKI-Software an Geräte erstellen.

Verbindung zwischen BlackBerry UEM und dem Entrust IdentityGuard-Server Ihrer Organisation mit Smart Credentials

Wenn Ihr Unternehmen von Entrust IdentityGuard verwaltete abgeleitete Smart Credentials verwendet, können Sie abgeleitete Smart Credentials auf Android-Geräten und in BlackBerry Dynamics-Apps auf iOS- und Android-Geräten verwenden.

Bevor Sie beginnen:

Wenden Sie sich an den Entrust-Administrator Ihrer Organisation, um folgende Informationen zu erhalten:

- URL des Entrust IdentityGuard-Servers
- Name der Smart Credential, die auf Geräten aktiviert werden soll, wie in Entrust IdentityGuard angegeben
- Entrust-Zertifizierungsstellenzertifikat zum Senden des Zertifikats an Geräte

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie auf **Externe Integration > Zertifizierungsstelle**.
3. Klicken Sie auf **Eine Verbindung für Entrust Smart Credentials hinzufügen**.
4. Geben Sie im Feld **Name für Smart Credential** den in Entrust IdentityGuard angegebenen Namen der Smart Credential ein.
5. Geben Sie im Feld **Entrust-URL** die URL des Entrust IdentityGuard-Servers ein.
6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Erstellen eines Profils mit Zertifizierungsstellenzertifikat um das Entrust-Zertifizierungsstellenzertifikat an Geräte zu senden und das Profil denselben Benutzern bzw. Gruppen zuzuweisen, denen das Profil für Benutzeranmeldeinformationen zugewiesen wird.
- Erstellen eines Profils mit Benutzeranmeldeinformationen zur Verwendung von Entrust Smart Credentials auf Geräten.

Herstellen einer Verbindung zwischen BlackBerry UEM und der OpenTrust-Software Ihrer Organisation

Um die zertifikatbasierte Authentifizierung von OpenTrust auf Geräten zu erweitern, müssen Sie eine Verbindung mit der OpenTrust-Software Ihrer Organisation hinzufügen. BlackBerry UEM unterstützt die Integration von OpenTrust PKI 4.8.0 und höher und OpenTrust CMS 2.0.4 und höher. Diese Verbindung wird von BlackBerry Dynamics-Apps nicht unterstützt.

Bevor Sie beginnen: Wenden Sie sich an den OpenTrust-Administrator Ihrer Organisation, um die URL des OpenTrust-Servers, das Clientzertifikat mit dem privaten Schlüssel (PFX- oder P12-Format) und das Zertifikatkennwort zu erhalten.

1. Klicken Sie in der Menüleiste auf **Einstellungen**.
2. Klicken Sie auf **Externe Integration > Zertifizierungsstelle**.
3. Klicken Sie auf **OpenTrust-Verbindung hinzufügen**.
4. Geben Sie im Feld **Verbindungsname** einen Namen für die Verbindung ein.
5. Geben Sie im Feld **URL** die URL für die OpenTrust-Software ein.
6. Klicken Sie auf **Durchsuchen**. Navigieren Sie zu dem clientseitigen Zertifikat, das BlackBerry UEM für die Verbindungsauthentifizierung mit dem OpenTrust-Server verwenden kann, und wählen Sie es aus.

7. Geben Sie im Feld **Zertifikatskennwort** das Kennwort für das OpenTrust-Serverzertifikat ein.
8. Um die Verbindung zu testen, klicken Sie auf **Verbindung testen**.
9. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Ein Profil mit Benutzeranmeldeinformationen zum Senden von Zertifikaten von Ihrer PKI-Software an Geräte erstellen.
- Wenn Sie die BlackBerry UEM-Verbindung mit der OpenTrust-Software zur Verteilung der Zertifikate auf Geräte verwenden, kann eine kurze Verzögerung auftreten, bevor die Zertifikate als gültig erkannt werden. Diese Verzögerung kann zu Problemen bei der E-Mail-Authentifizierung während des Vorgangs der Geräteaktivierung führen. Um dieses Problem zu beheben, konfigurieren Sie in der OpenTrust-Software die OpenTrust-Zertifizierungsstelle, und legen Sie „Zertifikate rückdatieren (Sekunden)“ auf 180 fest.

Verbindung von BlackBerry UEM mit einer BlackBerry Dynamics-PKI-Verbindung

Wenn Sie die PKI-Software Ihres Unternehmens zum Registrieren von Zertifikaten für BlackBerry Dynamics-Apps verwenden möchten und die PKI-Software eine direkte Verbindung zu BlackBerry UEM nicht unterstützt, können Sie eine BlackBerry Dynamics-PKI-Verbindung einrichten, um mit der Zertifizierungsstelle zu kommunizieren und BlackBerry UEM über die PKI-Verbindung zu verbinden.

Ein PKI-Konnektor besteht aus einer Reihe von Java-Programmen und Webdiensten auf einem Back-End-Server, der BlackBerry UEM das Senden von Zertifikatanfragen und das Empfangen von Antworten von der Zertifizierungsstelle ermöglicht. BlackBerry UEM verwendet das Benutzerzertifikat-Verwaltungsprotokoll von BlackBerry Dynamics für die Kommunikation mit dem PKI-Konnektor. Dieses Protokoll läuft über HTTPS und definiert Nachrichten im JSON-Format. Weitere Informationen zum Einrichten einer BlackBerry Dynamics-PKI-Verbindung finden Sie in der Dokumentation zum Benutzerzertifikat-Verwaltungsprotokoll und zur PKI-Verbindung.

Bevor Sie beginnen: Richten Sie eine BlackBerry Dynamics-PKI-Verbindung ein.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Zertifizierungsstelle**.
2. Klicken Sie auf **BlackBerry Dynamics PKI-Verbindung hinzufügen**.
3. Geben Sie im Feld **Verbindungsname** einen Namen für die Verbindung ein.
4. Geben Sie im Feld **URL** die URL für die PKI-Verbindung ein.
5. Wählen Sie eine der folgenden Optionen aus:
   - **Authentifizierung mit Benutzername und Kennwort**: Wählen Sie diese Option aus, wenn BlackBerry UEM die Authentifizierung mit der BlackBerry Dynamics-PKI-Verbindung mittels kennwortbasierter Authentifizierung durchführt.
   - **Authentifizierung mit Clientzertifikat**: Wählen Sie diese Option aus, wenn BlackBerry UEM die Authentifizierung mit der BlackBerry Dynamics-PKI-Verbindung mittels zertifikatsbasierter Authentifizierung durchführt.
6. Wenn Sie **Authentifizierung mit Benutzername und Kennwort** auswählen, geben Sie in die Felder **Benutzername** und **Kennwort** den Benutzernamen und das Kennwort für die BlackBerry Dynamics-PKI-Verbindung ein.
7. Wenn Sie **Authentifizierung mit Clientzertifikat** ausgewählt haben, klicken Sie auf **Durchsuchen**, um ein Zertifikat auszuwählen und hochzuladen, das von der BlackBerry Dynamics-PKI-Verbindung als vertrauenswürdig eingestuft wird. Geben Sie im Feld **Clientzertifikatskennwort** das Kennwort für das Zertifikat ein.

8. Im Abschnitt **Vertrauenswürdiges Zertifikat für die PKI-Verbindung** können Sie das Zertifikat angeben, das BlackBerry UEM verwendet, um Verbindungen mit der PKI-Verbindung zu vertrauen. Wählen Sie eine der folgenden Optionen aus:
   - **Zertifizierungsstellenzertifikat aus BlackBerry Control TrustStore**
   - **Zertifizierungsstellenzertifikat**: Wenn Sie diese Option auswählen, müssen Sie auf „Durchsuchen“ klicken, um zum Zertifizierungsstellenzertifikat Ihres Unternehmens zu navigieren und es auszuwählen.
   - **Serverzertifikat der PKI-Verbindung**: Wenn Sie diese Option auswählen, müssen Sie auf „Durchsuchen“ klicken, um zum Serverzertifikat der PKI-Verbindung Ihres Unternehmens zu navigieren und es auszuwählen.
9. Um die Verbindung zu testen, klicken Sie auf **Verbindung testen**.
10. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind:

- Ein Profil mit Benutzeranmeldeinformationen zum Senden von Zertifikaten von Ihrer PKI-Software an Geräte erstellen.

Herstellen einer Verbindung zwischen BlackBerry UEM und der App-basierten PKI-Lösung Ihrer Organisation

App-basierte PKI-Lösungen, wie z. B. Purebred umfassen eine auf einem Gerät installierte App, die mit einer Zertifizierungsstelle kommuniziert, um Zertifikate zu registrieren und zum Gerät hinzuzufügen. Sie können eine App-basierte PKI-Lösung verwenden, um Zertifikate zur Verwendung von BlackBerry Dynamics-Apps zur Verfügung zu stellen.

Zur Verwendung einer App-basierten PKI-Lösung mit iOS-Geräten müssen Sie eine Verbindung zwischen BlackBerry UEM und dem PKI-Anbieter hinzufügen. Für diese Aufgabe ist keine App-basierte PKI-Lösung nur mit Android-Geräten erforderlich.

Wenn die PKI-App, die die Zertifikate von der Zertifizierungsstelle abruft, keine BlackBerry Dynamics-App ist, kommuniziert der BlackBerry UEM Client mit der PKI-App, um die Zertifikate abzurufen und sie den BlackBerry Dynamics-Apps bereitzustellen.

Bevor Sie beginnen: Überprüfen Sie, ob die App zum Abrufen von Zertifikaten, die von BlackBerry Dynamics-Apps verwendet werden, in der App-Liste in BlackBerry UEM enthalten ist.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Externe Integration > Zertifizierungsstelle**.
2. Klicken Sie auf **Verbindung für gerätebasierte Zertifikate hinzufügen**.
3. Wählen Sie die App aus, die Zertifikate aus der PKI-App abruft, die von BlackBerry Dynamics-Apps verwendet werden. Wählen Sie BlackBerry UEM Client aus, um Purebred verwenden zu können.
4. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Erstellen von Profilen mit Anmeldeinformationen für App-basierte Zertifikate.
- Erstellen eines Profils mit Benutzeranmeldeinformationen zum Verwenden App-basierter Zertifikate auf iOS-Geräten.
- Erstellen eines Profils mit Benutzeranmeldeinformationen, um Zertifikate aus dem nativen Schlüsselspeicher auf Android-Geräten zu verwenden

Bereitstellen von Clientzertifikaten für Geräte und Apps

Sie und die Benutzer können Clientzertifikate auf verschiedene Arten an Geräte und Apps senden.

So wird das Zertifikat hinzugefügt	Beschreibung	Unterstützte Geräte
Während der Geräteaktivierung	BlackBerry UEM sendet während des Aktivierungsprozesses Zertifikate an Geräte. Die Geräte verwenden diese Zertifikate, um sichere Verbindungen zwischen dem Gerät und BlackBerry UEM herzustellen.	Alle
SCEP-Profile	Sie können SCEP-Profile erstellen, mit denen Geräte Verbindungen zu Clientzertifikaten herstellen und diese von der Zertifizierungsstelle Ihres Unternehmens mithilfe eines SCEP-Diensts abrufen. Die Geräte und BlackBerry Dynamics-Apps können diese Zertifikate für die zertifikatsbasierte Authentifizierung im Browser und für die Verbindung zu einem geschäftlichen Wi-Fi-Netzwerk, einem geschäftlichen VPN oder einem geschäftlichen Mailserver verwenden.	iOS macOS Android Windows 10 BlackBerry 10
Verbindung zur PKI-Lösung Ihres Unternehmens	Wenn Ihr Unternehmen eine PKI-Lösung, z. B. Entrust- oder OpenTrust-Softwareprodukte, verwendet, um Zertifikate auszustellen und zu verwalten, können Sie Profile für Benutzeranmeldeinformationen erstellen, die von Geräten verwendet werden, um Zertifikate von der Zertifizierungsstelle Ihres Unternehmens zu erhalten. Geräte mit BlackBerry Dynamics-Aktivierung verwenden diese Zertifikate für die zertifikatsbasierte Authentifizierung in BlackBerry Dynamics-Apps. Andere Geräte verwenden diese Zertifikate für die zertifikatsbasierte Authentifizierung im Browser und für die Verbindung zu einem geschäftlichen Wi-Fi-Netzwerk, einem geschäftlichen VPN oder einem geschäftlichen Mailserver.	iOS Android BlackBerry 10
Profile für freigegebenes Zertifikat	Ein Profil für ein freigegebenes Zertifikat legt ein Clientzertifikat fest, das BlackBerry UEM an iOS-, macOS- und Android-Geräte sendet. BlackBerry UEM sendet das gleiche Clientzertifikat an jeden Benutzer, dem das Profil zugewiesen ist. Der Administrator muss Zugriff auf das Zertifikat und den privaten Schlüssel haben, um ein Profil für ein freigegebenes Zertifikat zu erstellen.	iOS macOS Android

So wird das Zertifikat hinzugefügt	Beschreibung	Unterstützte Geräte
Senden von Clientzertifikaten an einzelne Benutzerkonten	Sie können einem Benutzerkonto ein Clientzertifikat hinzufügen. BlackBerry UEM kann das Zertifikat an die iOS- und Android-Geräte des Benutzers senden. Wenn das Zertifikat mit einem Profil für Benutzeranmeldeinformationen verknüpft ist, können Geräte diese Zertifikate verwenden, um eine Verbindung zu Ihrem geschäftlichen Wi-Fi-Netzwerk, geschäftlichen VPN oder geschäftlichen Mailserver herzustellen. Der Administrator muss Zugriff auf das Zertifikat und den privaten Schlüssel haben, um das Client-Zertifikat an den Benutzer zu senden.	iOS Android BlackBerry 10
Hochladen von Zertifikaten in UEM Self-Service durch Benutzer	Wenn Ihr Unternehmen über eine lokale BlackBerry UEM-Umgebung verfügt, können Benutzer Zertifikate in BlackBerry UEM Self-Service hochladen. BlackBerry UEM sendet das Zertifikat an die Geräte des Benutzers. Wenn das Zertifikat mit einem Profil für Benutzeranmeldeinformationen verknüpft ist, können Geräte und BlackBerry Dynamics-Apps diese Zertifikate verwenden, um auf ihrer Grundlage eine Authentifizierung durchzuführen und um eine Verbindung zu Ihrem geschäftlichen Wi-Fi-Netzwerk, geschäftlichen VPN oder geschäftlichen Mailserver herzustellen. Diese Funktion wird in BlackBerry UEM Cloud nicht unterstützt.	iOS Android BlackBerry 10
Benutzerimport	Auf BlackBerry 10-Geräten können Benutzer Clientzertifikate in den Zertifikatsspeicher des Geräts im Abschnitt „Sicherheit und Datenschutz“ der „Systemeinstellungen“ importieren. Zertifikate für die Verwendung im Arbeitsbrowser oder zum Senden von S/MIME-geschützten Nachrichten vom geschäftlichen E-Mail-Konto können aus dem Dateisystem auf dem Gerät oder aus einem Netzwerkpfad importiert werden, der vom geschäftlichen Bereich zugänglich ist. Auf Android-Geräten können Benutzer dem nativen Schlüsselspeicher des Geräts Zertifikate zur Verwendung mit BlackBerry Dynamics-Apps hinzufügen.	Android BlackBerry 10
Smartcards	Benutzer können S/MIME- und SSL-Zertifikate von einer Smartcard auf ihre Geräte importieren.	BlackBerry 10

Senden von Clientzertifikaten an Geräte und Apps mithilfe von Profilen

Sie können Zertifikate mithilfe der folgenden Profile, die in der Bibliothek der Richtlinien und Profile verfügbar sind, an Geräte und Apps senden:

Profil	Beschreibung
Zertifizierungsstellenzertifikat	Zertifizierungsstellenzertifikat-Profile legen ein Zertifizierungsstellenzertifikat fest, das jedes Client- oder Serverzertifikat als vertrauenswürdig zur Verwendung durch Geräte und BlackBerry Dynamics-Apps ausweist, das von der Zertifizierungsstelle signiert wurde.
Benutzeranmeldeinformationer	Profile für Benutzeranmeldeinformationen senden Zertifikate wie folgt an Geräte: • Sie legen fest, wie eine Verbindung zur PKI-Software Ihres Unternehmens hergestellt wird, um Clientzertifikate an Geräte und BlackBerry Dynamics-Apps zu senden. • Sie ermöglichen das manuelle Hochladen von Zertifikaten in BlackBerry UEM und ermöglichen in einer lokalen Umgebung Benutzern das Hochladen von Zertifikaten mit BlackBerry UEM Self-Service. • Sie können zulassen, dass BlackBerry Dynamics-Apps auf Android-Geräten Zertifikate aus dem nativen Schlüsselspeicher des Geräts verwenden. • Sie können BlackBerry Dynamics-Apps ermöglichen, Zertifikate von anderen App-basierten PKI-Lösungen wie z. B. Purebred zu importieren.
SCEP	SCEP-Profile geben an, wie Geräte und BlackBerry Dynamics-Apps Verbindungen zu Clientzertifikaten herstellen und diese von der Zertifizierungsstelle Ihres Unternehmens mithilfe eines SCEP-Diensts abrufen.
Freigegebenes Zertifikat	Profile für freigegebene Zertifikate legen ein Clientzertifikat fest, das BlackBerry UEM an iOS- und Android-Geräte sendet. BlackBerry UEM sendet das gleiche Clientzertifikat an jeden Benutzer, dem das Profil zugewiesen ist.

Für iOS- und Android-Geräte können Clientzertifikate auch an Geräte gesendet werden, indem sie einem Benutzerkonto hinzugefügt werden. Weitere Informationen finden Sie unter Hinzufügen eines Client-Zertifikats zu einem Benutzerkonto.

Für iOS- ‚Android- und BlackBerry 10-Geräte gilt: Wenn Ihr Unternehmen Zertifikate für S/MIME verwendet, können Sie auch Profile verwenden, um mit den Geräten öffentliche Schlüssel abzurufen und den Zertifikatstatus zu prüfen. Weitere Informationen finden Sie unter Erweitern der E-Mail-Sicherheit mithilfe von S/MIME.

Damit BlackBerry Dynamics-Apps von Profilen gesendete Zertifikate verwenden, wählen Sie „BlackBerry Dynamics-Apps die Verwendung von Benutzerzertifikaten, SCEP-Profilen und Benutzeranmeldeprofilen gestatten“ in den Einstellungen für die App aus.

Auswählen von Profilen, über die Clientzertifikate an Geräte und Apps gesendet werden sollen

Zum Senden von Clientzertifikaten an Geräte und BlackBerry Dynamics-Apps können Sie verschiedene Profiltypen verwenden. Die Auswahl des Profiltyps wird durch die Verwendungsart der Zertifikate in Ihrem Unternehmen und die von Ihrem Unternehmen unterstützten Gerätetypen bestimmt. Beachten Sie die folgenden Richtlinien:

- Für die Verwendung von SCEP-Profilen benötigen Sie eine Zertifizierungsstelle, die SCEP unterstützt.
- Wenn Sie eine Verbindung zwischen BlackBerry UEM und der PKI-Lösung Ihres Unternehmens eingerichtet haben, verwenden Sie Profile für Benutzeranmeldeinformationen, um Zertifikate an Geräte zu senden. Sie können direkt eine Verbindung zu einer Entrust-Zertifizierungsstelle oder OpenTrust-Zertifizierungsstelle herstellen. Sie können auch über eine BlackBerry Dynamics-PKI-Verbindung auf eine Zertifizierungsstelle zugreifen, um Zertifikate für BlackBerry Dynamics-fähige Geräte zu registrieren.
- Um Zertifikate mit BlackBerry Dynamics-Apps verwenden zu können, müssen Sie ein Profil mit Benutzeranmeldeinformationen verwenden oder die Zertifikate zu den einzelnen Benutzerkonten hinzufügen.
- Verwenden Sie ein Profil für Benutzeranmeldeinformationen, um Benutzern zu gestatten, Zertifikate hochzuladen und dann zur Verbindung mit Ihrem geschäftlichen Wi-Fi-Netzwerk, geschäftlichen VPN und geschäftlichen Mailserver zu verwenden.
- Um Clientzertifikate für die Wi-Fi-, VPN- und E-Mail-Server-Authentifizierung zu verwenden, müssen Sie das Zertifikatprofil mit einem Wi-Fi-, VPN- oder E-Mail-Profil verknüpfen.

  Hinweis: Android Enterprise-Geräte unterstützen keine Zertifikate, die über BlackBerry UEM für die Wi-Fi - Authentifizierung an Geräte gesendet werden.
- Bei Profilen mit freigegebenem Zertifikat und Zertifikaten, die Benutzerkonten hinzugefügt werden, werden private Schlüssel nicht geheim gehalten, weil Sie Zugriff auf den privaten Schlüssel benötigen. Der Zugriff auf eine Zertifizierungsstelle über SCEP oder Profile für Benutzeranmeldeinformationen ist sicherer, da der private Schlüssel nur an das Gerät gesendet wird, für das das Zertifikat ausgestellt wurde.

Senden von Zertifizierungsstellenzertifikaten an Geräte und Apps

Sie müssen möglicherweise Zertifizierungsstellenzertifikate an Geräte senden, wenn Ihr Unternehmen S/MIME verwendet oder wenn Geräte oder BlackBerry Dynamics-Apps eine zertifikatsbasierte Authentifizierung für die Verbindung mit einem Netzwerk oder einem Server in Ihrer Unternehmensumgebung verwenden.

Wenn ein Zertifizierungsstellenzertifikat auf einem Gerät gespeichert wird, vertrauen das Gerät und die Apps dem mit einem von der Zertifizierungsstelle erstellten Cyber- oder Serverzertifikat. Wenn die von der Zertifizierungsstelle ausgegebenen Netzwerk- und Serverzertifikate Ihrer Organisation auf Geräten gespeichert werden, ist die Vertrauenswürdigkeit beim Aufbau sicherer Verbindungen zu Ihren Netzwerken und Servern gewährleistet. Wenn das Zertifizierungsstellenzertifikat, das die S/MIME-Zertifikate Ihrer Organisation unterzeichnet hat, auf Geräten gespeichert wird, kann der E-Mail-Client dem Zertifikat des Senders vertrauen, wenn eine sichere E-Mail eingeht.

Es können mehrere Zertifizierungsstellenzertifikate für verschiedene Zwecke auf einem Gerät gespeichert werden. Mithilfe von Profilen mit Zertifizierungsstellenzertifikat können Sie Zertifizierungsstellenzertifikate an Geräte senden.

Erstellen eines Profils mit Zertifizierungsstellenzertifikat

Bevor Sie beginnen: Beziehen Sie die Zertifizierungsstellen-Zertifikatdatei von Ihrem PKI-Administrator.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Zertifizierungsstellenzertifikat**.

3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil mit Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen. Einige Namen (z. B. ca_1) sind reserviert.
5. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
6. Wenn das Zertifizierungsstellenzertifikat an BlackBerry 10-Geräte gesendet wird, geben Sie auf der Registerkarte BlackBerry einen oder mehrere der folgenden Zertifikatspeicher an, um das Zertifikat an das Gerät zu senden:
   - Browser-Zertifikatspeicher
   - VPN-Zertifikatspeicher
   - Wi-Fi-Zertifikatspeicher
   - Unternehmens-Zertifikatspeicher
7. Wenn das Zertifizierungsstellenzertifikat an macOS-Geräte gesendet wird, wählen Sie auf der Registerkarte macOS in der Dropdown-Liste **Profil anwenden auf** den Eintrag **Benutzer** oder **Gerät** aus.
8. Klicken Sie auf **Hinzufügen**.

Speicher für Zertifizierungsstellenzertifikate auf BlackBerry 10-Geräten

Zertifizierungsstellenzertifikate, die an BlackBerry 10-Geräte gesendet werden, können je nach dem Zweck in unterschiedlichen Zertifikatspeichern gespeichert werden.

Speicher	Beschreibung
Browser-Zertifikatspeicher	Der geschäftliche Browser auf BlackBerry 10-Geräten nutzt die Zertifikate in diesem Speicher, um SSL-Verbindungen zu Servern in Ihrer Unternehmensumgebung herzustellen.
VPN-Zertifikatspeicher	BlackBerry 10-Geräte nutzen Zertifikate in diesem Speicher für VPN-Verbindungen. Sie müssen die Einstellung „Quelle des vertrauenswürdigen Zertifikats“ im VPN-Profil auf „Speicher vertrauenswürdiger Zertifikate“ festlegen, um die Zertifikate in diesem Speicher für geschäftliche VPN-Verbindungen nutzen zu können.
Wi-Fi-Zertifikatspeicher	BlackBerry 10-Geräte nutzen Zertifikate in diesem Speicher für Wi-Fi-Verbindungen. Sie müssen die Einstellung „Quelle des vertrauenswürdigen Zertifikats“ im Wi-Fi-Profil auf „Speicher vertrauenswürdiger Zertifikate“ festlegen, um die Zertifikate in diesem Speicher für Wi-Fi-Geschäftsverbindungen nutzen zu können.
Unternehmens-Zertifikatspeicher	BlackBerry 10-Geräte nutzen die Zertifikate in diesem Speicher, um eingehende S/MIME-geschützte E-Mail-Nachrichten zu authentifizieren.

Senden von Clientzertifikaten an Geräte und Apps unter Verwendung von Profilen für Benutzeranmeldeinformationen

Profile für Benutzeranmeldeinformationen ermöglichen es Geräten, Kundenzertifikate zu verwenden, die anhand der folgenden Methoden abgerufen wurden:

- Manuelles Hochladen von Zertifikaten in die BlackBerry UEM-Verwaltungskonsole oder, in einer lokalen Umgebung, in BlackBerry UEM Self-Service

- Eine bestehende Verbindung zwischen BlackBerry UEM und der Entrust-Zertifizierungsstelle oder OpenTrust-Zertifizierungsstelle Ihres Unternehmens
- Für BlackBerry Dynamics-Apps auf Android-Geräten, im nativen Schlüsselspeicher gespeicherte Zertifikate
- Für BlackBerry Dynamics-Apps, über eine bestehende BlackBerry Dynamics-PKI-Anschlussverbindung
- Für BlackBerry Dynamics-Apps, mit einer App-basierten PKI-Lösung wie Purebred.

Wenn Benutzer Zertifikate in UEM Self-Service manuell hochladen, wird das Zertifikat auf der Benutzerseite der Verwaltungskonsole angezeigt. Sie können das Zertifikat zudem löschen oder ersetzen. Diese Funktion wird in BlackBerry UEM Cloud nicht unterstützt.

Profile für Benutzeranmeldeinformationen werden auf iOS- und Android-Geräten sowie auf Geräten mit BlackBerry 10 OS Version 10.3.1 und höher unterstützt. App-basierte PKI-Lösungen werden für BlackBerry Dynamics-Apps auf iOS- und Android-Geräten unterstützt. Manuelles Hochladen von Zertifikaten wird für iOS-, Android Enterprise-, Samsung Knox Workspace- und BlackBerry 10-Geräte unterstützt.

Weitere Informationen zum Verbinden von BlackBerry UEM mit der PKI-Software Ihres Unternehmens finden Sie unter Vernetzung von BlackBerry UEM und der PKI-Software Ihrer Organisation.

Alternativ kann die Registrierung von Clientzertifikaten auf Geräten auch über SCEP-Profile erfolgen. Sie können Zertifikate auch direkt in ein Benutzerkonto hochladen. Der ausgewählte Profiltyp hängt von der Verwendungsart der PKI-Software, den von Ihrem Unternehmen unterstützten Geräten und den zu verwaltenden Zertifikaten ab.

Profil mit Benutzeranmeldeinformationen zum manuellen Hochladen von Zertifikaten erstellen

Mithilfe von Profilen mit Benutzeranmeldeinformationen können Sie oder Benutzer Zertifikate, die an Benutzergeräte gesendet werden sollen, manuell hochladen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Benutzeranmeldeinformationen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Wählen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** die Option **Manuell hochgeladenes Zertifikat** aus.
6. Wenn Sie Android Enterprise-Geräte verwalten und Benutzer daran hindern möchten, das Zertifikat für andere Zwecke auszuwählen, wählen Sie auf der Registerkarte **Android** die Option **Zertifikat auf Android Enterprise-Geräten ausblenden** aus. Diese Option gilt nur für Geräte mit Android 9.0 und höher.
7. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Wenn Geräte Clientzertifikate zur Authentifizierung bei einem Wi-Fi-Netzwerk, VPN oder Mailserver verwenden, verknüpfen Sie das Profil für Benutzeranmeldeinformationen mit einem Wi-Fi-, VPN- oder E-Mail-Profil.
- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.
- Hinzufügen eines Client-Zertifikats zu einem Profil mit Benutzeranmeldeinformationen oder weisen Sie Benutzer an, BlackBerry UEM Self-Service zum Hochladen ihres eigenen Zertifikats zu verwenden.

Erstellen eines Profils für Benutzeranmeldeinformationen zur Verbindung mit der PKI-Software Ihres Unternehmens

Profile für Benutzeranmeldeinformationen, die eine Verbindung zur PKI-Software Ihres Unternehmens herstellen, können Zertifikate für iOS-, Android- und BlackBerry 10 OS-Geräte mit Version 10.3.1 und höher registrieren. Wenn die Verbindung zur Entrust-PKI-Software besteht, kann das Profil für Benutzeranmeldeinformationen auch Zertifikate für BlackBerry Dynamics-Apps registrieren.

Hinweis: BlackBerry UEM unterstützt keinen Schlüsselverlauf für Zertifikate, die für BlackBerry Dynamics-Apps ausgestellt wurden.

Bevor Sie beginnen:

- Konfigurieren Sie eine Verbindung zur Entrust oder OpenTrust Software Ihres Unternehmens.
- Kontaktieren Sie den Entrust- oder OpenTrust-Administrator Ihres Unternehmens, um zu klären, welches PKI-Profil Sie auswählen sollten. BlackBerry UEM erhält eine Liste der Profile von der PKI-Software.
- Fragen Sie den Entrust- oder OpenTrust-Administrator nach den Profilwerten, die Sie angeben müssen. Beispielsweise die Werte für Gerätetypen (devicetype), Entrust IdentityGuard-Gruppen (iggroup) und Entrust IdentityGuard-Benutzernamen (igusername).
- Wenn das OpenTrust-System Ihrer Organisation nur zur Rückgabe von Escrowed-Schlüsseln konfiguriert ist, muss der OpenTrust-Administrator sicherstellen, dass für jeden Benutzer im OpenTrust-System Zertifikate vorhanden sind. Wenn Sie Benutzern in BlackBerry UEM ein Profil für Benutzeranmeldedaten zuweisen, werden die Zertifikate für Benutzer in OpenTrust nicht automatisch erstellt. In diesem Szenario können über das Profil für Benutzeranmeldedaten nur Zertifikate an Benutzer verteilt werden, die ein bestehendes Zertifikat im OpenTrust-System aufweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Benutzeranmeldeinformationen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Wählen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** die von Ihnen konfigurierte Entrust- oder OpenTrust-Verbindung.
6. Klicken Sie in der Dropdown-Liste **Profil** auf das entsprechende Profil.
7. Geben Sie die Werte für das Profil an.
8. Bei Bedarf können Sie den SAN-Typ und -Wert des alternativen Antragstellers für ein Entrust-Clientzertifikat angeben.
   a) Klicken Sie in der SAN-Tabelle auf +.
   b) Klicken Sie in der Dropdown-Liste **SAN-Typ** auf den entsprechenden Typ.
   c) Geben Sie im Feld **SAN-Wert** den SAN-Wert ein.

   Wenn „RFC 822-Name“ als SAN-Typ festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn „URI“ festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn „NT-Prinzipalname“ festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn „DNS-Name“ festgelegt ist, muss der Wert ein gültiger FQDN sein.
9. Geben Sie den **Erneuerungszeitraum** des Zertifikats ein. Der Zeitraum kann zwischen 1 und 120 Tagen betragen.
10. Wenn BlackBerry 10-Geräte für die Verschlüsselung von E-Mail-Nachrichten mittels S/MIME Clientzertifikate verwenden und der Zugriff auf abgelaufene Zertifikate beibehalten werden soll, sodass Benutzer ältere E-Mail-Nachrichten weiterhin öffnen können, aktivieren Sie das Kontrollkästchen **Zertifikatsverlauf einschließen**.
11. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Wenn Geräte Clientzertifikate zur Authentifizierung bei einem Wi-Fi-Netzwerk, VPN oder Mailserver verwenden, verknüpfen Sie das Profil für Benutzeranmeldeinformationen mit einem Wi-Fi-, VPN- oder E-Mail-Profil.
- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu. Android-Benutzer werden beim Empfang des Profils zur Eingabe eines Kennworts aufgefordert (das Kennwort wird auf dem Bildschirm angezeigt).

Erstellen eines Profils mit Benutzeranmeldeinformationen zur Verwendung von Entrust Smart Credentials auf Geräten

Entrust abgeleitete Smart Credentials werden von den folgenden Apps unterstützt:

- BlackBerry Dynamics-Apps auf iOS-Geräten
- BlackBerry Dynamics-Apps auf anderen Android-Geräten als Samsung Knox Workspace-Geräten
- Apps auf Android Enterprise-Geräten, die Zertifikate für Signatur, Verschlüsselung und Identitätsauthentifizierung verwenden, wie z. B. BlackBerry Hub und unterstützte Webbrowser
- Apps auf Samsung Knox Workspace-Geräten, die Zertifikate für Signatur, Verschlüsselung und Identitätsauthentifizierung verwenden, wie z. B. Samsung nativer E-Mail-Client und unterstützte Webbrowser

Hinweis: BlackBerry UEM unterstützt keinen Schlüsselverlauf für abgeleitete Smart Credentials.

Bevor Sie beginnen:

- Verbindung zwischen BlackBerry UEM und dem Entrust IdentityGuard-Server Ihrer Organisation mit Smart Credentials.
- Erstellen eines Profils mit Zertifizierungsstellenzertifikat um das Zertifizierungsstellenzertifikat von Entrust an Geräte zu senden und das Profil denselben Benutzern oder Gruppen zuzuweisen, denen dieses Profil mit Benutzeranmeldeinformationen zugewiesen ist.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Benutzeranmeldeinformationen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Klicken Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** auf die Entrust Smart Credential-Verbindung, die Sie konfiguriert haben.
6. Geben Sie in der Dropdown-Liste **Zertifikattyp** an, ob Smart Credentials für die Identitätsauthentifizierung, Signatur oder Verschlüsselung verwendet werden sollen.

   Wenn Sie Smart Credentials für mehrere Zwecke an Apps senden möchten, erstellen Sie zusätzliche Profile mit Benutzeranmeldeinformationen.
7. Wenn die Smart Credentials an Samsung Knox Workspace-Geräte oder andere Apps als die BlackBerry Dynamics-Apps auf Android Enterprise-Geräten gesendet werden, klicken Sie auf die Registerkarte **Android**, und wählen Sie **An systemeigene Schlüsselkette bereitstellen** aus.

   Wenn diese Einstellung nicht ausgewählt ist, können die Smart Credentials nur von BlackBerry Dynamics-Apps verwendet werden.
8. Wenn die Smart Credentials an BlackBerry Dynamics-Apps gesendet werden, klicken Sie auf die Registerkarte **BlackBerry Dynamics**, und führen Sie die folgenden Schritte aus:
   a) Wenn das Gerät doppelte Anmeldedaten löschen soll, wählen Sie **Doppelte Zertifikate löschen**. Das Gerät löscht die Anmeldedaten mit dem frühesten Startdatum.
   b) Wenn das Gerät abgelaufene Anmeldedaten löschen soll, wählen Sie **Abgelaufene Zertifikate löschen**.
   c) Damit alle BlackBerry Dynamics-Apps die Smart Credentials verwenden können, wählen Sie **Allen Apps erlauben, Zertifikate zu verwenden** aus.
   d) Um die BlackBerry Dynamics-Apps anzugeben, die die Smart Credentials verwenden sollen, wählen Sie die Option **Bestimmten Apps erlauben, Zertifikate zu verwenden** aus, und klicken Sie auf +, um die Apps anzugeben. Sie müssen BlackBerry UEM Client in die Liste der Apps aufnehmen.
9. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.

- Nachdem ein Gerät das Profil empfangen hat, müssen sich Benutzer beim Entrust IdentityGuard Self-Service-Modul anmelden, um ihre Smart Credentials zu aktivieren, und den BlackBerry UEM Client verwenden, um den vom Entrust IdentityGuard Self-Service-Modul angezeigten QR-Code zu scannen und die Smart Credentials zum Gerät hinzuzufügen.
- Um Entrust Smart Credentials von einem Gerät zu entfernen, sollte der Benutzer die Smart Credentials im BlackBerry UEM Client deaktivieren, bevor Sie die Zuweisung des Profils aufheben oder das Zertifikat entfernen.

Erstellen eines Profils mit Benutzeranmeldeinformationen, um Zertifikate aus dem nativen Schlüsselspeicher auf Android-Geräten zu verwenden

Sie können das Benutzerzertifikatprofil so konfigurieren, dass BlackBerry Dynamics-Apps ein Zertifikat aus dem nativen Schlüsselspeicher auf Android-Geräten verwenden können. Sie können zulassen, dass BlackBerry Dynamics-Apps jedes Zertifikat verwenden, das dem Schlüsselspeicher hinzugefügt wurde, oder Sie können Einschränkungen dafür definieren, welches Zertifikat die App auswählen kann. Wenn Sie z. B. eine App-basierte PKI-Lösung wie Purebred verwenden, die Zertifikate zum nativen Schlüsselspeicher hinzufügt, können Sie die App zwingen, ein von Ihrer Purebred-PKI-Lösung ausgestelltes Zertifikat auszuwählen und Zertifikate mit bestimmten Funktionen zu verwenden.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Benutzeranmeldeinformationen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Wählen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** die Option **Nativer Schlüsselspeicher** aus.
6. Um anzugeben, welches Zertifikat die BlackBerry Dynamics-App verwenden soll, führen Sie die folgenden Aktionen durch:
   a) Klicken Sie neben **Aussteller** auf +, und geben Sie den Ausstellernamen ein.

      BlackBerry Dynamics-Apps verwenden nur dann ein Zertifikat, wenn der angegebene Aussteller mit der OpenSSL-Kurzform-OID im Zertifikat übereinstimmt. Sie können diesen Wert aus dem Zertifikat des Ausstellers kopieren. Fügen Sie vor oder nach einem Gleichheitszeichen (=) keine Leerstellen ein. Beispiel:

      ```
      CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                CN=Acme_cert TLS
      ```

   b) Wählen Sie im Abschnitt **Schlüsselnutzung** die Vorgänge aus, die das Zertifikat unterstützt.

      BlackBerry Dynamics-Apps verwenden nur Zertifikate, für die mindestens der angegebene Schlüsselnutzungswert festgelegt ist. Ein Verschlüsselungszertifikat kann beispielsweise den Schlüsselnutzungswert **Schlüsselverschlüsselung** aufweisen. Ein Authentifizierungszertifikat kann den Schlüsselnutzungswert **Digitale Signatur** aufweisen. Ein Signaturzertifikat kann den Schlüsselnutzungswert **Digitale Signatur** und **Zugelassen** aufweisen.
   c) Wählen Sie im Abschnitt **Erweiterte Schlüsselnutzung** die Funktionen aus, für die das Zertifikat ausgestellt wurde.

      BlackBerry Dynamics-Apps verwenden nur dann Zertifikate, wenn alle ausgewählten erweiterten Schlüsselnutzungswerte im Zertifikat vorhanden sind. Zertifikate können über zusätzliche erweiterte Schlüsselnutzungswerte verfügen.
   d) Wenn das Zertifikat für andere Zwecke als E-Mail, Client-Authentifizierung oder Smartcard-Anmeldung ausgestellt wurde, wählen Sie **Zusätzliche Verwendung der Objekt-ID** aus, klicken Sie auf +, und geben Sie die OID für die Schlüsselnutzung an. Wenn das Zertifikat beispielsweise für die Serverauthentifizierung verwendet wird, kann es die OID 1.3.6.1.5.5.7.3.1 aufweisen.

7. Wenn das Gerät abgelaufene Zertifikate löschen soll, wählen Sie **Abgelaufene Zertifikate löschen**.

   Abgelaufene Verschlüsselungszertifikate für S/MIME sollten auf dem Gerät aufbewahrt werden, um Benutzern das Lesen von Nachrichten zu ermöglichen, die vor Ablauf des Zertifikats verschlüsselt wurden.
8. Wenn das Gerät doppelte Zertifikate löschen soll, wählen Sie **Doppeltes Zertifikat entfernen**. Das Gerät löscht das Zertifikat mit dem frühesten Startdatum.
9. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Zulassen, dass BlackBerry Dynamics-Apps Zertifikate verwenden.
- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.

Erstellen eines Profils für Benutzeranmeldeinformationen zur Verbindung mit Ihrer BlackBerry Dynamics-PKI-Software

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Benutzeranmeldeinformationen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Klicken Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** auf die von Ihnen konfigurierte BlackBerry Dynamics-PKI-Verbindung.
6. Wenn der Benutzer ein Kennwort zur Anforderung eines Zertifikats angeben muss, wählen Sie **Vom Benutzer eingegebenes Kennwort oder OTP anfordern** aus.
7. Wenn das Gerät automatisch ein neues Zertifikat anfordern soll, bevor das aktuelle Zertifikat abläuft, wählen Sie **Zertifikaterneuerung aktivieren**, und geben Sie die Anzahl der Tage vor dem Ablaufdatum an, um festzulegen, wann das Gerät ein neues Zertifikat anfordert.
8. Wenn das Gerät abgelaufene Zertifikate löschen soll, wählen Sie **Abgelaufene Zertifikate löschen**.
9. Wenn das Gerät doppelte Zertifikate löschen soll, wählen Sie **Doppeltes Zertifikat entfernen**. Das Gerät löscht das Zertifikat mit dem frühesten Startdatum.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Zulassen, dass BlackBerry Dynamics-Apps Zertifikate verwenden.
- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.
- Wenn Sie die PKI-Connector aktualisieren, klicken Sie auf **PKI-Funktionen aktualisieren**, um die unterstützten PKI-Funktionen für das Profil zu aktualisieren.

Erneuern von Zertifikaten, die über den PKI-Connector für BlackBerry Dynamics registriert wurden

Wenn Sie Benutzerzertifikate für alle BlackBerry Dynamics-Benutzer aktualisieren, können Sie einen Befehl zum Anfordern einer Zertifikatverlängerung für alle Geräte senden, die dem Profil mit Benutzeranmeldeinformationen zugewiesen sind.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Benutzeranmeldeinformationen**.
3. Klicken Sie auf den Namen des Profils, das Sie ändern möchten.
4. Klicken Sie auf **PKI-Funktionen aktualisieren**, um sicherzustellen, dass BlackBerry UEM die aktuellsten Informationen für den PKI-Connector aufweist.

5. Klicken Sie auf **Erneuern**, um die Zertifikaterneuerung für alle BlackBerry Dynamics-fähigen Geräte anzufordern, denen das Profil zugewiesen ist.

Erstellen von Profilen mit Anmeldeinformationen für App-basierte Zertifikate

App-basierte PKI-Lösungen, wie z. B. Purebred umfassen eine auf einem Gerät installierte App, die mit einer Zertifizierungsstelle kommuniziert, um Zertifikate zu registrieren und zum Gerät hinzuzufügen. Sie können eine App-basierte PKI-Lösung verwenden, um Zertifikate zur Verwendung von BlackBerry Dynamics-Apps zur Verfügung zu stellen.

Zur Verwendung einer App-basierten PKI-Lösung mit iOS-Geräten müssen Sie eine Verbindung zwischen BlackBerry UEM und dem PKI-Anbieter hinzufügen. Für diese Aufgabe ist keine App-basierte PKI-Lösung nur mit Android-Geräten erforderlich.

Wenn die PKI-App, die die Zertifikate von der Zertifizierungsstelle abruft, keine BlackBerry Dynamics-App ist, kommuniziert der BlackBerry UEM Client mit der PKI-App, um die Zertifikate abzurufen und sie den BlackBerry Dynamics-Apps bereitzustellen.

Wenn Sie mehrere Zertifikate mit dieser Methode an Geräte senden, wird empfohlen, mehrere Profile für Benutzeranmeldeinformationen einzurichten, wobei jedes Profil einen anderen Zertifikattyp verwendet. Wenn Sie eine einzige Profilinstanz für mehrere Zertifikate verwenden, wird nicht angegeben, ob Zertifikate fehlen. Wenn ein Profil zum Beispiel separate Verschlüsselungs-, Signatur- und Authentifizierungszertifikate enthält und nur die Signatur- und Authentifizierungszertifikate importiert werden, wird auf dem Gerät angezeigt, dass der Import erfolgreich war, obwohl das Verschlüsselungszertifikat fehlt. Wenn Sie jedoch drei separate Profile für Benutzeranmeldeinformationen einrichten und das Verschlüsselungszertifikat fehlt, ist der Fehler offensichtlich.

Schritte zur Verwendung App-basierter Zertifikate

Einige der Schritte, die zur Verwendung der anwendungsbasierten PKI-Lösung Ihres Unternehmens erforderlich sind, sind nur erforderlich, wenn Sie die Lösung mit iOS-Geräten verwenden.

Schritt	Aktion
1	Um eine anwendungsbasierte PKI-Lösung mit iOS-Geräten zu verwenden, wählen Sie im BlackBerry Dynamics-Profil die Option **Anmeldung des UEM Client bei BlackBerry Dynamics aktivieren**, und legen Sie BlackBerry UEM Client für die **Delegierung der App-Authentifizierung** fest.
2	Wenn Sie eine anwendungsbasierte PKI-Lösung mit iOS-Geräten verwenden möchten, stellen Sie eine Verbindung zwischen BlackBerry UEM und der anwendungsbasierten PKI-Lösung Ihres Unternehmens her.
3	Wenn Sie eine anwendungsbasierte PKI-Lösung mit iOS-Geräten verwenden möchten und die PKI-App keine BlackBerry Dynamics-Anwendung ist, konfigurieren Sie BlackBerry UEM Client so, dass anwendungsbasierte Zertifikate unterstützt werden.
4	Konfigurieren Sie BlackBerry Dynamics-Apps für die Verwendung App-basierter Zertifikate.
5	Stellen Sie sicher, dass die PKI-App (z. B. Purebred) auf den Geräten der Benutzer installiert ist.
6	Um die anwendungsbasierte PKI-Lösung mit iOS-Geräten zu verwenden, erstellen Sie ein Benutzeranmeldungsprofil für die Verwendung App-basierter Zertifikate.

Schritt	Aktion
7	Um die anwendungsbasierte PKI-Lösung mit Android-Geräten zu verwenden, erstellen Sie ein Benutzeranmeldungsprofil für die Verwendung von Zertifikaten aus dem nativen Schlüsselspeicher.

Konfigurieren von BlackBerry UEM Client zur Unterstützung von App-basierten Zertifikaten

Diese Aufgabe ist nur erforderlich, wenn Sie die App-basierte PKI-Lösung Ihres Unternehmens mit iOS-Geräten verwenden und die PKI-App keine BlackBerry Dynamics-App ist.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**.
2. Wählen Sie in der App-Liste BlackBerry UEM Client aus.
3. Klicken Sie im Abschnitt VPN-Konfiguration auf +.
4. Geben Sie im Feld **App-Name** den Namen der App ein.
5. Geben Sie im Feld **UTI-Schemata** die UTI-Schemata für die App-basierte PKI-Lösung Ihres Unternehmens an. Wenn Sie die Purebred-App nutzen, verwenden Sie beispielsweise die folgenden Schemata: purebred.zip.all, purebred.zip.no_filter.
6. Klicken Sie auf **Speichern**.
7. Weisen Sie BlackBerry UEM Client mit der von Ihnen erstellten App-Konfiguration den Benutzern und Geräten zu, die die App-basierte PKI-Lösung verwenden sollen.

Konfigurieren von BlackBerry Dynamics-Apps für die Verwendung App-basierter Zertifikate

BlackBerry Dynamics-Apps wählen automatisch aus, welches Zertifikat für S/MIME und für die Authentifizierung über TLS-Verbindungen basierend auf der Schlüsselverwendung und den Eigenschaften der erweiterten Schlüsselnutzung in den Zertifikaten verwendet werden soll. Wenn zwei oder mehr Zertifikate dieselben Eigenschaften aufweisen, können Apps möglicherweise nicht auflösen, welches Zertifikat für die TLS-Authentifizierung verwendet werden soll. Führen Sie die folgenden Schritte aus, um Apps bei der Bestimmung des zu verwendenden Zertifikats zu helfen.

1. Klicken Sie in der Menüleiste der BlackBerry UEM-Verwaltungskonsole auf **Apps**.
2. Wählen Sie die App in der App-Liste aus (z. B. BlackBerry Work oder BlackBerry Access).
3. Wählen Sie die Option **BlackBerry Dynamics-Apps die Verwendung von Benutzerzertifikaten und Profilen für Benutzeranmeldeinformationen gestatten** aus.
4. Wenn Sie BlackBerry Work konfigurieren, klicken Sie im Konfigurationsabschnitt auf +, und führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Konfigurieren von BlackBerry Work, wenn Ihr Unternehmen BEMS verwendet	a. Wählen Sie auf der Registerkarte „Konfigurationseinstellungen“ **Clients müssen über individuelle Anmeldezertifikate verfügen (SSL), die in GC hochgeladen werden** aus. b. Zum Aktivieren der automatischen Erkennung des Microsoft Exchange-Servers, auf dem sich die Benutzer befinden, wählen Sie **BEMS für die automatische Erkennung des EAS/EWS-Endpunkt des Benutzers verwenden** aus. c. Geben Sie auf der Registerkarte **Exchange-Einstellungen** im Feld **Profilname für die Benutzeranmeldeinformationen** den Namen des Profils für die Benutzeranmeldeinformationen ein.

Aufgabe	Schritte
Konfigurieren von BlackBerry Work, wenn Ihr Unternehmen BEMS nicht verwendet	**a.** Wählen Sie die Registerkarte **Exchange-Einstellungen** aus. **b.** Wenn Ihr Server das Anmeldeformat *Domänenname\Benutzer* verwendet, geben Sie im Feld **Standarddomäne** die Windows NT-Standarddomäne ein, mit der BlackBerry Work eine Verbindung herstellt, wenn sich Benutzer anmelden. **c.** Geben Sie im Feld **Aktiver Sync-Server** den Exchange ActiveSync-Standardserver an, mit dem BlackBerry Work eine Verbindung herstellt, wenn sich Benutzer bei BlackBerry Work anmelden (z. B. cas.mydomain.com). **d.** Geben Sie im Feld **Automatische Erkennungs-URL** die URL für die automatische Erkennung an, falls diese bekannt ist. Damit wird der Prozess für die Einrichtung der automatischen Erkennung beschleunigt (z. B. https://autodiscover.mydomain.com). **e.** Geben Sie im Feld **Verbindungs-Timeout der automatischen Erkennung in Sekunden (nur iOS)** das Timeout für die automatische Erkennung der Verbindung in Sekunden an. **f.** Geben Sie im Feld **Profilname für die Benutzeranmeldeinformationen** den Namen des Profils für die Benutzeranmeldeinformationen ein.

5. Klicken Sie auf **Speichern**.

Erstellen eines Profils mit Benutzeranmeldeinformationen zum Verwenden App-basierter Zertifikate auf iOS-Geräten

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikate > Benutzeranmeldeinformationen**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Wählen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** den Namen der App aus, die Sie beim Herstellen der Verbindung zwischen BlackBerry UEM und Ihrer PKI-Lösung angegeben haben. Wenn Sie Purebred verwenden, wählen Sie den BlackBerry UEM Client aus.
6. Um anzugeben, welches Zertifikat die BlackBerry Dynamics-App verwenden soll, führen Sie die folgenden Aktionen durch:
   a) Wählen Sie im Abschnitt **Schlüsselnutzung** die Vorgänge aus, die das Zertifikat unterstützt.

      BlackBerry Dynamics-Apps verwenden nur Zertifikate, für die mindestens der angegebene Schlüsselnutzungswert festgelegt ist. Ein Verschlüsselungszertifikat kann beispielsweise den Schlüsselnutzungswert **Schlüsselverschlüsselung** aufweisen. Ein Authentifizierungszertifikat kann den Schlüsselnutzungswert **Digitale Signatur** aufweisen. Ein Signaturzertifikat kann den Schlüsselnutzungswert **Digitale Signatur** und **Zugelassen** aufweisen.
   b) Wählen Sie im Abschnitt **Erweiterte Schlüsselnutzung** die Funktionen aus, für die das Zertifikat ausgestellt wurde.

      BlackBerry Dynamics-Apps verwenden nur dann Zertifikate, wenn alle ausgewählten erweiterten Schlüsselnutzungswerte im Zertifikat vorhanden sind. Zertifikate können über zusätzliche erweiterte Schlüsselnutzungswerte verfügen.
   c) Wenn das Zertifikat für andere Zwecke als E-Mail, Client-Authentifizierung oder Smartcard-Anmeldung ausgestellt wurde, wählen Sie **Zusätzliche Verwendung der Objekt-ID** aus, klicken Sie auf +, und geben Sie die OID für die Schlüsselnutzung an. Wenn das Zertifikat beispielsweise für die Serverauthentifizierung verwendet wird, kann es die OID 1.3.6.1.5.5.7.3.1 aufweisen.

d) Klicken Sie neben **Aussteller** auf +, und geben Sie den Ausstellernamen ein.

BlackBerry Dynamics-Apps verwenden nur dann ein Zertifikat, wenn der angegebene Aussteller mit der OpenSSL-Kurzform-OID im Zertifikat übereinstimmt. Sie können diesen Wert aus dem Zertifikat des Ausstellers kopieren. Fügen Sie vor oder nach dem Gleichheitszeichen (=) keine Leerstellen ein. Beispiel:

```
CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme,C=Can
                                        CN=Acme_cert SMIME,OU=Acme_Legal,O=Acme
                                        CN=Acme_cert TLS
```

7. Wenn das Gerät abgelaufene Zertifikate löschen soll, wählen Sie **Abgelaufene Zertifikate löschen**.

   Abgelaufene Verschlüsselungszertifikate für S/MIME sollten auf dem Gerät aufbewahrt werden, um Benutzern das Lesen von Nachrichten zu ermöglichen, die vor Ablauf des Zertifikats verschlüsselt wurden.
8. Wenn das Gerät doppelte Zertifikate löschen soll, wählen Sie **Doppeltes Zertifikat entfernen**. Das Gerät löscht das Zertifikat mit dem frühesten Startdatum.
9. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Zulassen, dass BlackBerry Dynamics-Apps Zertifikate verwenden.
- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.

Senden von Clientzertifikaten an Geräte und Apps mithilfe von SCEP

Sie können SCEP-Profile verwenden, um anzugeben, wie Geräte und BlackBerry Dynamics-Apps Clientzertifikate über einen SCEP-Dienst aus der Zertifizierungsstelle Ihres Unternehmens abrufen. SCEP ist ein IETF-Protokoll, das das Anmelden von Client-Zertifikaten auf vielen Geräten oder in vielen Anwendungen vereinfacht, indem zur Ausstellung der einzelnen Zertifikate weder ein Eingriff vonseiten des Administrators noch eine Genehmigung erforderlich ist. Geräte und BlackBerry Dynamics-Apps können SCEP verwenden, um Client-Zertifikate von einer SCEP-kompatiblen Zertifizierungsstelle, die Ihr Unternehmen verwendet, anzufordern und abzurufen.

Die von Ihnen verwendete Zertifizierungsstelle muss Challenge-Kennwörter unterstützen. Die Zertifizierungsstelle verifiziert mithilfe von Challenge-Kennwörtern, dass das Gerät oder die App zum Senden einer Zertifikatsanforderung autorisiert ist.

Für die Verwendung von SCEP in einer BlackBerry UEM Cloud-Umgebung ist die Installation der neuesten Version von BlackBerry Connectivity Node erforderlich, damit BlackBerry UEM Cloud auf Ihr Firmenverzeichnis zugreifen kann.

Wenn Ihr Unternehmen eine Entrust- oder OpenTrust-Zertifizierungsstelle verwendet, werden SCEP-Profile für Windows 10-Geräte nicht unterstützt.

Erstellen eines SCEP-Profils

Die erforderlichen Profileinstellungen hängen von der SCEP-Servicekonfiguration in der Umgebung Ihres Unternehmens ab und variieren je nachdem, ob das Zertifikat von einer BlackBerry Dynamics-App oder von einem bestimmten Gerätetyp verwendet wird.

Sie können eine Variable in einem beliebigen Textfeld verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben.

Hinweis: Wenn Sie ein SCEP-Profil zur Verteilung von OpenTrust-Clientzertifikaten auf Geräten verwenden, müssen Sie einen Hotfix auf die OpenTrust-Software anwenden. Um weitere Informationen zu erhalten, wenden Sie sich bitte an Ihren OpenTrust-Kundendienstmitarbeiter, und verweisen Sie auf Support-Fall SUPPORT-798.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.

2. Klicken Sie auf **Zertifikate > SCEP**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Führen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** eine der folgenden Aktionen aus:
   - Um eine von Ihnen konfigurierte Entrust-Verbindung zu verwenden, klicken Sie auf die entsprechende Verbindung. Klicken Sie in der Dropdown-Liste **Profil** auf ein Profil. Geben Sie die Werte für das Profil an.
   - Um eine von Ihnen konfigurierte OpenTrust-Verbindung zu verwenden, klicken Sie auf die entsprechende Verbindung. Klicken Sie in der Dropdown-Liste **Profil** auf ein Profil. Geben Sie die Werte für das Profil an.
     - Die folgenden Einstellungen im SCEP-Profil gelten nicht für die OpenTrust-Clientzertifikate: Schlüsselnutzung, Erweiterte Schlüsselnutzung, Antragsteller und SAN.
   - Um eine andere Zertifizierungsstelle zu verwenden, klicken Sie auf **Generisch**. Wählen Sie in der Dropdown-Liste **SCEP-Abfragetyp** entweder **Statisch** oder **Dynamisch** aus, und geben Sie die erforderlichen Einstellungen für den Abfragetyp an.

     Hinweis: Für Windows-Geräte werden nur „statische“ Kennwörter unterstützt.
6. Geben Sie im Feld **URL** die URL für den SCEP-Dienst ein. Die URL sollte das Protokoll, den FQDN, die Portnummer und den SCEP-Pfad enthalten.
7. Geben Sie im Feld **Instanzname** den Instanznamen der Zertifizierungsstelle ein.
8. Deaktivieren Sie optional das Kontrollkästchen für alle Gerätetypen, für die Sie das Profil nicht konfigurieren möchten.
9. Führen Sie folgende Aktionen aus:
   a) Klicken Sie auf die Registerkarte eines Gerätetyps.
   b) Konfigurieren Sie die entsprechenden Werte für jede Profileinstellung so, dass sie der SCEP-Dienstkonfiguration in der Umgebung Ihres Unternehmens entsprechen.
10. Wiederholen Sie Schritt 8 für jeden Gerätetyp in Ihrer Organisation.
11. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Wenn Geräte das Clientzertifikat zur Authentifizierung bei einem geschäftlichen Wi-Fi-Netzwerk, geschäftlichen VPN oder einem geschäftlichen Mailserver verwenden, verknüpfen Sie das SCEP-Profil mit einem Wi-Fi-, VPN- oder E-Mail-Profil.

SCEP-Profileinstellungen

SCEP-Profile werden auf den folgenden Gerätetypen unterstützt:

- iOS
- macOS
- Android
- Windows 10
- BlackBerry 10

Allgemein: SCEP-Profileinstellungen

Allgemein: SCEP-Profileinstellung	Beschreibung
Zertifizierungsstellenverbindung	Diese Einstellung gibt an, ob es sich bei der Zertifizierungsstelle um eine Entrust-, OpenTrust- oder eine andere Zertifizierungsstelle handelt. Wenn Sie eine oder mehrere Verbindungen in der Entrust- oder OpenTrust-Software Ihrer Organisation konfiguriert haben, können Sie eine der Verbindungen in der Dropdown-Liste auswählen. Wählen Sie „Generisch“ aus, wenn Sie eine beliebige andere Zertifizierungsstelle verwenden. Wenn Sie eine Entrust oder OpenTrust-Verbindung auswählen, müssen Sie anschließend das passende PKI-Profil auswählen und die erforderlichen Werte angeben. Die verfügbaren Profile variieren je nach Konfiguration der PKI-Software durch den Entrust- oder OpenTrust-Administrator. Der Standardwert ist „Generisch“.
URL	Diese Einstellung legt die URL für den SCEP-Dienst fest. Die URL sollte das Protokoll, den FQDN, die Portnummer und den SCEP-Pfad (CGI-Pfad, der in der SCEP-Spezifikation definiert wurde) enthalten. Sie müssen einen Wert für diese Einstellung festlegen, um ein Gerät erfolgreich zu aktivieren. SCEP-HTTPS-URLs werden von iOS-Geräten und BlackBerry 10 OS Version 10.3.0 und höher unterstützt.
Instanzenname	Diese Einstellung legt den Namen der Zertifizierungsstelleninstanz fest. Der Wert kann jede beliebige Zeichenkette sein, die der SCEP-Dienst versteht. So könnte der Wert beispielsweise ein Domänenname wie etwa „Beispiel.org“ sein. Wenn eine Zertifizierungsstelle mehrere Zertifizierungsstellenzertifikate aufweist, kann anhand dieses Feldes festgelegt werden, welches dieser Zertifikate verwendet wird.
Die Vertrauenskette der SCEP-Serververbindung überprüfen	Diese Einstellung gibt an, ob BlackBerry UEM im BlackBerry UEM-Zertifikatspeicher nach der Stammzertifizierungsstelle des SCEP-Servers sucht, um für BlackBerry UEM die Vertrauenswürdigkeit des SCEP-Servers beim Testen von Verbindungen, beim Abrufen von Challenge-Kennwörtern und als Proxy für SCEP-Anforderungen von Geräten zu überprüfen.
SCEP-Abfragetyp	Diese Einstellung legt fest, ob das SCEP-Abfragekennwort dynamisch generiert oder als statisches Kennwort bereitgestellt wird. Wenn diese Einstellung auf „Statisch“ gesetzt ist, verwenden alle Geräte das gleiche Abfragekennwort. Wenn diese Einstellung auf „Dynamisch“ gesetzt ist, verwendet jedes Gerät ein eindeutiges Kennwort. Mögliche Werte: • Statisch • Dynamisch Der Standardwert ist „Dynamisch“. Für Windows-Geräte werden nur „statische“ Kennwörter unterstützt.

Allgemein: SCEP-Profileinstellung	Beschreibung
URL der Challenge-Kennwortgenerierung	Diese Einstellung legt die URL fest, die Geräte verwenden, um ein dynamisch generiertes Abfragekennwort vom SCEP-Dienst abzurufen. Die URL sollte das Protokoll, den FQDN, die Portnummer und den SCEP-Pfad (CGI-Pfad, der in der SCEP-Spezifikation definiert wurde) enthalten. Wenn Sie ein dynamisches Abfragekennwort verwenden, müssen Sie einen Wert für diese Einstellung festlegen, um BlackBerry 10-Geräte erfolgreich zu aktivieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp fest, den Geräte verwenden, um eine Verbindung zum SCEP-Dienst aufzubauen und ein Abfragekennwort abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist. Mögliche Werte: • Einfach • NTLM Der Standardwert ist „Einfach“.
Domäne	Diese Einstellung legt die Domäne fest, die für die NTLM-Authentifizierung verwendet wird, wenn Geräte eine Verbindung zum SCEP-Dienst aufbauen, um ein Abfragekennwort abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „NTLM“ gesetzt ist.
Benutzername	Diese Einstellung legt den Benutzernamen fest, der zum Abrufen eines Abfragekennworts vom SCEP-Dienst erforderlich ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, das erforderlich ist, um das Abfragekennwort vom SCEP-Dienst abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Dynamisch“ gesetzt ist.
Challenge-Kennwort	Diese Einstellung legt das Abfragekennwort fest, das ein Gerät für die Zertifikatsanmeldung verwendet. Wenn Sie ein statisches Abfragekennwort verwenden, müssen Sie einen Wert für diese Einstellung festlegen, um BlackBerry 10-Geräte erfolgreich zu aktivieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SCEP-Abfragetyp“ auf „Statisch“ gesetzt ist.

iOS: SCEP-Profileinstellungen

iOS: SCEP-Profileinstellung	Beschreibung
BlackBerry UEM als Proxy für SCEP-Anforderungen verwenden	Diese Einstellung legt fest, ob alle SCEP-Anforderungen von Geräten per BlackBerry UEM gesendet werden. Wenn sich die Zertifizierungsstelle hinter Ihrer Firewall befindet, können Sie mithilfe dieser Einstellung Clientzertifikate auf Geräten anmelden, ohne die Zertifizierungsstelle außerhalb der Firewall sichtbar zu machen.
BlackBerry Connectivity Node für CA-Konnektivität verwenden	Diese Einstellung gibt an, ob SCEP-Anforderungen per BlackBerry Connectivity Node weitergeleitet werden sollen. Diese Einstellung wird nur in BlackBerry UEM Cloud angezeigt.
Empfänger	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, empfiehlt sich das Verwenden einer Variable wie „%UserDistinguishedName%“.
Wiederholungen	Diese Einstellung legt fest, wie oft der Verbindungsaufbau zum SCEP-Dienst wiederholt wird, wenn der erste Verbindungsversuch fehlgeschlagen ist. Mögliche Werte sind 1 bis 999. Der Standardwert ist „3“.
Wiederholungsverzögerung	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen. Mögliche Werte sind 1 bis 999. Der Standardwert ist 10 Sekunden.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest. Mögliche Werte: • 1024 • 2048 Der Standardwert ist 1024.
Fingerabdruck	Diese Einstellung legt den Fingerabdruck für das Anmelden eines SCEP-Zertifikats fest. Wenn Ihre Zertifizierungsstelle mit HTTP anstelle von HTTPS arbeitet, verwenden Geräte den Fingerabdruck, um die Identität der Zertifizierungsstelle beim Anmeldevorgang zu bestätigen. Der Fingerabdruck darf keine Leerräume aufweisen.

iOS: SCEP-Profileinstellung	Beschreibung
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • Keine • RFC 822-Name • DNS-Name • Uniform Resource Identifier (Einheitlicher Ressourcenbezeichner) Der Standardwert ist „Keine“.
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Zertifikatempfängers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle oder die vollqualifizierte URL des Servers sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn „RFC 822-Name“ festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn „URI“ festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn „NT-Prinzipalname“ festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn „DNS-Name“ festgelegt ist, muss der Wert ein gültiger FQDN sein.
NT-Prinzipalname	Diese Einstellung legt den NT-Prinzipalnamen für die Zertifikatsgenerierung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SAN-Typ“ auf etwas anderes als „Keine“ gesetzt ist.
Profilgültigkeit	Geben Sie die Anzahl der Tage an, nach denen ein Gerät nach dem Ausstellen eines Zertifikats ein neues Zertifikat von der Zertifizierungsstelle anfordert. Der Wert sollte kleiner sein als der Gültigkeitszeitraum des Zertifikats, der durch die CA definiert wird. Der Höchstwert beträgt 1825 Tage.

macOS: SCEP-Profileinstellungen

Bei macOS gelten Profile für Benutzerkonten oder Geräte. Sie können SCEP-Profile konfigurieren, die entweder für Benutzerkonten oder für Geräte gelten.

macOS: SCEP-Profileinstellung	Beschreibung
BlackBerry UEM als Proxy für SCEP-Anforderungen verwenden	Diese Einstellung legt fest, ob alle SCEP-Anforderungen von Geräten per BlackBerry UEM gesendet werden. Wenn sich die Zertifizierungsstelle hinter Ihrer Firewall befindet, können Sie mithilfe dieser Einstellung Clientzertifikate auf Geräten anmelden, ohne die Zertifizierungsstelle außerhalb der Firewall sichtbar zu machen.
BlackBerry Connectivity Node für CA-Konnektivität verwenden	Diese Einstellung gibt an, ob SCEP-Anforderungen per BlackBerry Connectivity Node weitergeleitet werden sollen. Diese Einstellung wird nur in BlackBerry UEM Cloud angezeigt.

macOS: SCEP-Profileinstellung	Beschreibung
Profil anwenden auf	Diese Einstellung gibt an, ob das SCEP-Profil für das Benutzerkonto oder das Gerät gilt. Mögliche Werte: • Benutzer • Gerät
Empfänger	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, empfiehlt sich das Verwenden einer Variable wie „%UserDistinguishedName%“.
Wiederholungen	Diese Einstellung legt fest, wie oft der Verbindungsaufbau zum SCEP-Dienst wiederholt wird, wenn der erste Verbindungsversuch fehlgeschlagen ist. Mögliche Werte sind 1 bis 999. Der Standardwert ist „3“.
Wiederholungsverzögerung	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen. Mögliche Werte sind 1 bis 999. Der Standardwert ist 10 Sekunden.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest. Mögliche Werte: • 1024 • 2048 Der Standardwert ist „1024“.
Fingerabdruck	Diese Einstellung legt den Fingerabdruck für das Anmelden eines SCEP-Zertifikats fest. Wenn Ihre Zertifizierungsstelle mit HTTP anstelle von HTTPS arbeitet, verwenden Geräte den Fingerabdruck, um die Identität der Zertifizierungsstelle beim Anmeldevorgang zu bestätigen. Der Fingerabdruck darf keine Leerräume aufweisen.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • Keine • RFC 822-Name • DNS-Name • Uniform Resource Identifier (Einheitlicher Ressourcenbezeichner) Der Standardwert ist „Keine“.

macOS: SCEP-Profileinstellung	Beschreibung
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Zertifikatempfängers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle oder die vollqualifizierte URL des Servers sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn „RFC 822-Name“ festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn „URI“ festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn „NT-Prinzipalname“ festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn „DNS-Name“ festgelegt ist, muss der Wert ein gültiger FQDN sein.
NT-Prinzipalname	Diese Einstellung legt den NT-Prinzipalnamen für die Zertifikatsgenerierung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „SAN-Typ“ auf etwas anderes als „Keine“ gesetzt ist.

Android: SCEP-Profileinstellungen

Ein Beispiel eines SCEP-Profils für Android-Geräte finden Sie in Artikel 38248 unter support.blackberry.com/community.

Android: SCEP-Profileinstellung	Beschreibung
BlackBerry UEM als Proxy für SCEP-Anforderungen verwenden	Diese Einstellung legt fest, ob alle SCEP-Anforderungen von Geräten per BlackBerry UEM gesendet werden. Wenn sich die Zertifizierungsstelle hinter Ihrer Firewall befindet, können Sie mithilfe dieser Einstellung Clientzertifikate auf Geräten anmelden, ohne die Zertifizierungsstelle außerhalb der Firewall sichtbar zu machen.
Ausblenden des Zertifikats auf Android Enterprise-Geräten	Diese Einstellung legt fest, ob das Zertifikat für Benutzer ab Android Version 9.0 Android Enterprise sichtbar ist. Wenn das Zertifikat ausgeblendet ist, können Benutzer das Zertifikat nicht für zusätzliche Zwecke auswählen.
BlackBerry Connectivity Node für CA-Konnektivität verwenden	Diese Einstellung gibt an, ob SCEP-Anforderungen per BlackBerry Connectivity Node weitergeleitet werden sollen. Diese Einstellung wird nur in BlackBerry UEM Cloud angezeigt.
Verschlüsselungsalgorithm	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, den Android-Geräte für die Zertifikatsanmeldungsanforderung verwenden. Mögliche Werte: • Keine • Triple DES • AES (128-Bit) • AES (196-Bit) • AES (256-Bit) Der Standardwert ist „Triple DES“.

Android: SCEP-Profileinstellung	Beschreibung
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die Android-Geräte für die Zertifikatsanmeldungsanforderung verwenden. Mögliche Werte: • Keine • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „SHA-1“.
Fingerabdruck des Zertifikats	Diese Einstellung legt den hexadezimal-codierten Hash des Stammzertifikats für die Zertifizierungsstelle fest. Sie können folgende Algorithmen verwenden, um den Fingerabdruck festzulegen: SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512. Sie müssen einen Wert für diese Einstellung festlegen, um Android Enterprise- oder Samsung Knox-Geräte zu aktivieren.
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll. Mögliche Werte sind 1 bis 365. Der Standardwert ist „30“.
Android Enterprise/Samsung KNOX	
Empfänger	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, empfiehlt sich das Verwenden einer Variable wie „%UserDistinguishedName%“.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • RFC 822-Name • Uniform Resource Identifier • NT-Prinzipalname • DNS-Name Der Standardwert ist „RFC 822-Name“.

Android: SCEP-Profileinstellung	Beschreibung
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Antragstellers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle, die vollqualifizierte URL des Servers oder ein Prinzipalname sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn „RFC 822-Name“ festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn „URI“ festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn „NT-Prinzipalname“ festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn „DNS-Name“ festgelegt ist, muss der Wert ein gültiger FQDN sein.
Schlüsselalgorithmus	Diese Einstellung legt den Algorithmus fest, den Android Enterprise- und Samsung Knox-Geräte verwenden, um das Client-Schlüsselpaar zu generieren. Sie müssen einen Algorithmus auswählen, der von Ihrer Zertifizierungsstelle unterstützt wird. Mögliche Werte: • Keine • RSA • ECC Der Standardwert ist „RSA“.
RSA-Stärke	Diese Einstellung legt die RSA-Stärke fest, die Android Enterprise- und Samsung Knox-Geräte verwenden, um das Client-Schlüsselpaar zu generieren. Sie müssen eine Schlüsselstärke eingeben, die von Ihrer Zertifizierungsstelle unterstützt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Schlüsselalgorithmus“ auf „RSA“ gesetzt ist. Mögliche Werte: • 1024 • 2048 • 4096 • 8192 • 16384 Der Standardwert ist „1024“.

Android: SCEP-Profileinstellung	Beschreibung
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können. Mögliche Auswahlen: • Digitale Signatur • Nichtabstreitbarkeit • Schlüsselverschlüsselung • Datenverschlüsselung • Schlüsselvereinbarung • Schlüsselzertifikat-Signierung • CRL-Signierung • Nur verschlüsseln • Nur entschlüsseln Die Standardauswahlen lauten „Digital Signatur“, „Schlüsselverschlüsselung“ und „Schlüsselvereinbarung“.
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an. Mögliche Auswahlen: • Server-Authentifizierung • Client-Authentifizierung • Codesignierung • E-Mail-Schutz • Zeitstempel • OCSP-Signierung • Secure Shell Client • Secure Shell Server Die Standardauswahl lautet „Client-Authentifizierung“.

Windows 10: SCEP-Profileinstellungen

Windows 10: SCEP-Profileinstellung	Beschreibung
Speicher für Benutzerzertifikate	Diese Einstellung legt fest, ob das Zertifikat am Speicherort für Benutzerzertifikate auf dem Gerät gespeichert werden soll.
Empfänger	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, empfiehlt sich das Verwenden einer Variable wie „%UserDistinguishedName%“.

Windows 10: SCEP-Profileinstellung	Beschreibung
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • Keine • RFC 822-Name • DNS-Name • Uniform Resource Identifier Der Standardwert ist „Keine“.
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Zertifikatempfängers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle oder die vollqualifizierte URL des Servers sein. Welcher Wert für diese Einstellung geeignet ist, hängt von dem Wert ab, der für die Einstellung „SAN-Typ“ gewählt wurde.
Wiederholungen	Diese Einstellung legt fest, wie oft der Verbindungsaufbau zum SCEP-Dienst wiederholt wird, wenn der erste Verbindungsversuch fehlgeschlagen ist. Mögliche Werte sind 1 bis 999. Der Standardwert ist „3“.
Wiederholungsverzögerung	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen. Mögliche Werte sind 1 bis 999. Der Standardwert ist 10 Sekunden.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest. Mögliche Werte: • 1024 • 2048 • 4096 • 8192 • 16384 Der Standardwert ist „1024“.

Windows 10: SCEP-Profileinstellung	Beschreibung
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können. • Digitale Signatur • Nichtabstreitbarkeit • Schlüsselverschlüsselung • Datenverschlüsselung • Schlüsselvereinbarung • Schlüsselzertifikat-Signierung • CRL-Signierung • Nur verschlüsseln Die Standardauswahl ist „Schlüsselzertifikat-Signierung“ und „Nur verschlüsseln“.
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an. • Server-Authentifizierung • Client-Authentifizierung • Codesignierung • E-Mail-Schutz • Zeitstempel • OCSP-Signierung • Secure Shell Client • Secure Shell Server Die Standardauswahl lautet „Client-Authentifizierung“.
SCEP-Schlüsselspeicher	Diese Einstellung gibt den Speicherort für den privaten Schlüssel an. Mögliche Werte: • TPM • TPM, wenn unterstützt • KSP Der Standardwert ist „KSP“.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die ein Windows 10-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „SHA-1“.

Windows 10: SCEP-Profileinstellung	Beschreibung
Fingerabdruck des Zertifikats	Diese Einstellung legt den hexadezimal-codierten Hash des Stammzertifikats für die Zertifizierungsstelle fest. Sie können folgende Algorithmen verwenden, um den Fingerabdruck festzulegen: SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512.
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll. Mögliche Werte sind 1 bis 365. Der Standardwert ist „30“.

BlackBerry 10: SCEP-Profileinstellungen

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
Standard-Antragsteller und SAN verwenden	Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät den Namen des Antragstellers und den alternativen Antragstellernamen für eine Zertifikatsanforderung generiert. Wenn die Einstellung nicht ausgewählt wird, müssen Sie den Antragsteller und den Namenstyp und -wert des alternativen Antragstellers angeben.
Empfänger	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>/O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, empfiehlt sich das Verwenden einer Variable wie „%UserDistinguishedName%“. Diese Einstellung ist nur gültig, wenn „Standard-Antragsteller und SAN verwenden“ nicht ausgewählt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
SAN	Diese Einstellung gibt den Namenstyp und -wert des alternativen Antragstellers für ein Zertifikat an. Diese Einstellung ist nur gültig, wenn „Standard-Antragsteller und SAN verwenden“ nicht ausgewählt ist. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • RFC 822-Name • URI • NT-Prinzipalname • DNS-Name Der Standardwert ist „RFC 822-Name“.

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Antragstellers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle, die vollqualifizierte URL des Servers oder ein Prinzipalname sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn „RFC 822-Name“ festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn „URI“ festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn „NT-Prinzipalname“ festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn „DNS-Name“ festgelegt ist, muss der Wert ein gültiger FQDN sein.
Schlüsselalgorithmus	Diese Einstellung legt den Algorithmus fest, den ein BlackBerry 10-Gerät verwendet, um das Client-Schlüsselpaar zu generieren. Sie müssen einen Algorithmus auswählen, der von Ihrer Zertifizierungsstelle unterstützt wird. Mögliche Werte: • Keine • RSA • ECC Der Standardwert ist „RSA“.
RSA-Stärke	Diese Einstellung legt die RSA-Stärke fest, die ein BlackBerry 10-Gerät verwendet, um das Client-Schlüsselpaar zu generieren. Sie müssen eine Schlüsselstärke eingeben, die von Ihrer Zertifizierungsstelle unterstützt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Schlüsselalgorithmus“ auf „RSA“ gesetzt ist. Mögliche Werte: • 1024 • 2048 • 4096 • 8192 • 16384 Der Standardwert ist „1024“.

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
ECC-Stärke	Diese Einstellung legt die elliptische Kurve fest, die ein BlackBerry 10-Gerät verwendet, um ein Client-Schlüsselpaar zu generieren. Die elliptische Kurve definiert die Stärke des Client-Schlüsselpaars. Sie müssen eine elliptische Kurve auswählen, die von Ihrer Zertifizierungsstelle unterstützt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Schlüsselalgorithmus“ auf „ECC“ gesetzt ist. Mögliche Werte: • sect163k1 • sect283k1 • secp192r1 • secp256r1 • secp384r1 • secp521r1 Der Standardwert ist „secp521r1“.
Verschlüsselungsalgorithmus	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, den ein BlackBerry 10-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • Triple DES • AES (128-Bit) • AES (196-Bit) • AES (256-Bit) Der Standardwert ist „Triple DES“.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die ein BlackBerry 10-Gerät für die Zertifikatsanmeldungsanforderung verwendet. Mögliche Werte: • Keine • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „SHA-1“.
Fingerabdruck des Zertifikats	Diese Einstellung legt den hexadezimal-codierten Hash des Stammzertifikats für die Zertifizierungsstelle fest. Sie können folgende Algorithmen verwenden, um den Fingerabdruck festzulegen: MD5, SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512. Sie müssen einen Wert für diese Einstellung festlegen, um ein BlackBerry 10-Gerät erfolgreich zu aktivieren.

BlackBerry 10: SCEP-Profileinstellung	Beschreibung
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll. Mögliche Werte sind 1 bis 999.999.999 Tage. Der Standardwert ist „30“.
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können. Mögliche Auswahlen: • Digitale Signatur • Nichtabstreitbarkeit • Schlüsselverschlüsselung • Datenverschlüsselung • Schlüsselvereinbarung • Schlüsselzertifikat-Signierung • CRL-Signierung • Nur verschlüsseln • Nur entschlüsseln Die Standardauswahlen lauten „Digital Signatur“, „Schlüsselverschlüsselung“ und „Schlüsselvereinbarung“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an. Mögliche Auswahlen: • Server-Authentifizierung • Client-Authentifizierung • Codesignierung • E-Mail-Schutz • Zeitstempel • OCSP-Signierung • Secure Shell Client • Secure Shell Server Die Standardauswahl lautet „Client-Authentifizierung“. Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.

BlackBerry Dynamics: SCEP-Profileinstellungen

Diese Einstellungen gelten für SCEP-Zertifikate, die mit BlackBerry Dynamics-Apps auf iOS- und Android-Geräten verwendet werden.

BlackBerry Dynamics: SCEP-Profileinstellung	Beschreibung
Empfänger	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff in folgendem Format ein: „/CN=<*common_name*>,O=<*domain_name*>“. Wenn das Profil für mehrere Benutzer eingerichtet wird, empfiehlt sich das Verwenden einer Variable wie „%UserDistinguishedName%“.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest. Mögliche Werte: • RFC 822-Name • Uniform Resource Identifier • NT-Prinzipalname • DNS-Name Der Standardwert ist „RFC 822-Name“.
SAN-Wert	Diese Einstellung legt die alternative Darstellung des Antragstellers fest. Der Wert muss eine E-Mail-Adresse, der DNS-Name des Servers der Zertifizierungsstelle, die vollqualifizierte URL des Servers oder ein Prinzipalname sein. Die Einstellung „SAN-Typ“ bestimmt den Typ des geeigneten Werts, der angegeben werden muss. Wenn „RFC 822-Name“ festgelegt ist, muss der Wert eine gültige E-Mail-Adresse sein. Wenn „URI“ festgelegt ist, muss der Wert eine gültige URL sein, die das Protokoll und den FQDN oder die IP-Adresse enthält. Wenn „NT-Prinzipalname“ festgelegt ist, muss der Wert ein gültiger Prinzipalname sein. Wenn „DNS-Name“ festgelegt ist, muss der Wert ein gültiger FQDN sein.
Schlüsselalgorithmus	Diese Einstellung legt den Algorithmus fest, der zum Generieren des Client-Schlüsselpaars verwendet wird. Sie müssen einen Algorithmus auswählen, der von Ihrer Zertifizierungsstelle unterstützt wird. Mögliche Werte: • RSA
RSA-Stärke	Diese Einstellung legt die RSA-Stärke fest, die zum Generieren des Client-Schlüsselpaars verwendet wird. Sie müssen eine Schlüsselstärke eingeben, die von Ihrer Zertifizierungsstelle unterstützt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Schlüsselalgorithmus“ auf „RSA“ gesetzt ist. Mögliche Werte: • 2048 • 4096 Der Standardwert ist „2048“.

BlackBerry Dynamics: SCEP-Profileinstellung	Beschreibung
Verschlüsselungsalgorithm	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, der für die Zertifikatsanmeldungsanforderung verwendet wird. Mögliche Werte: • Triple DES • AES (128-Bit) • AES (196-Bit) • AES (256-Bit) Der Standardwert ist „Triple DES“.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die für die Zertifikatsanmeldungsanforderung verwendet wird. Mögliche Werte: • SHA-256 • SHA-384 • SHA-512 Der Standardwert ist „SHA-256“.
Fingerabdruck des Zertifikats	Diese Einstellung legt den hexadezimal-codierten Hash des Stammzertifikats für die Zertifizierungsstelle fest. Sie können einen der folgenden Algorithmen verwenden, um den Fingerabdruck festzulegen: SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512. MD5 wird nur unterstützt, wenn „FIPS aktivieren“ im BlackBerry Dynamics-Profil nicht ausgewählt ist.
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll. Mögliche Werte sind 1 bis 365. Der Standardwert ist „30“.
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können. Mögliche Auswahlen: • Digitale Signatur • Nichtabstreitbarkeit • Schlüsselverschlüsselung • Datenverschlüsselung • Schlüsselvereinbarung • Schlüsselzertifikat-Signierung • CRL-Signierung • Nur verschlüsseln • Nur entschlüsseln Die Standardauswahlen lauten „Digital Signatur“, „Schlüsselverschlüsselung“ und „Schlüsselvereinbarung“.

BlackBerry Dynamics: SCEP-Profileinstellung	Beschreibung
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an. Mögliche Auswahlen: • Server-Authentifizierung • Client-Authentifizierung • Codesignierung • E-Mail-Schutz • Zeitstempel • OCSP-Signierung • Secure Shell Client • Secure Shell Server Die Standardauswahl lautet „Client-Authentifizierung“.
App-Einschränkungen	Diese Einstellung gibt an, welche BlackBerry Dynamics-Apps das Zertifikat verwenden können. Mögliche Werte: • Allen Apps erlauben, Zertifikate zu verwenden • Bestimmten Apps erlauben, Zertifikate zu verwenden Die Standardauswahl lautet „Allen Apps erlauben, Zertifikate zu verwenden“.
Apps, die SCEP verwenden dürfen	Diese Einstellung gibt an, welche BlackBerry Dynamics-Apps die SCEP-Zertifikate verwenden dürfen. Diese Einstellung ist nur gültig, wenn die Einstellung „App-Einschränkungen“ auf „Bestimmten Apps erlauben, Zertifikate zu verwenden“ gesetzt ist.
Abgelaufene Zertifikate löschen	Diese Einstellung legt fest, ob das Gerät abgelaufene Zertifikate löscht.
Doppelte Zertifikate entfernen	Diese Einstellung legt fest, ob das Gerät doppelte Zertifikate löscht. Das Gerät löscht das Zertifikat mit dem frühesten Startdatum.

Senden des gleichen Clientzertifikats an mehrere Geräte

Sie können Profile für freigegebene Zertifikate verwenden, um Clientzertifikate an iOS-, macOS- und Android-Geräte zu senden.

Profile für freigegebene Zertifikate senden das gleiche Schlüsselpaar an jeden Benutzer, dem das Profil zugeordnet ist. Sie sollten Profile für freigegebene Zertifikate nur dann nutzen, wenn Sie mehr als einem Benutzer die gemeinsame Nutzung eines Client-Zertifikats ermöglichen möchten.

Bei macOS gelten Profile für Benutzerkonten oder Geräte. Sie können Profile für freigegebene Zertifikate konfigurieren, die entweder für Benutzerkonten oder Geräte gelten.

Erstellen eines Profils für ein freigegebenes Zertifikat

Bevor Sie beginnen: Sie müssen die Client-Zertifikatdatei abrufen, die Sie an die Geräte senden möchten. Die Zertifikatdatei muss die Dateierweiterung .pfx oder .p12 aufweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Zertifikat > Freigegebenes Zertifikat**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen. Einige Namen (z. B. ca_1) sind reserviert.
5. Geben Sie im Feld **Kennwort** ein Kennwort für das Profil des freigegebenen Zertifikats ein.
6. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
7. Wenn Sie Android Enterprise-Geräte verwalten und Benutzer daran hindern möchten, das Zertifikat für andere Zwecke auszuwählen, wählen Sie auf der Registerkarte **Android** die Option **Zertifikat auf Android Enterprise-Geräten ausblenden** aus. Diese Option gilt nur für Geräte mit Android 9.0 und höher.
8. Wenn Sie macOS-Geräte verwalten, wählen Sie auf der Registerkarte **macOS** in der Dropdown-Liste **Profil anwenden auf** den Eintrag **Benutzer** oder **Gerät** aus.
9. Klicken Sie auf **Hinzufügen**.

Angabe des von einer App verwendeten Zertifikats

Für Android-Geräte können Sie ein Zertifikatzuordnungsprofil verwenden, um die von Apps verwendeten Clientzertifikate anzugeben. Das Zertifikatzuordnungsprofil wird nicht für BlackBerry Dynamics-Apps unterstützt.

Mit Zertifikatzuordnungsprofilen können Sie die Zertifikate angeben, die von Android-Apps verwendet werden. Sie können festlegen, dass eine App ein von einem SCEP gesendetes Zertifikat, Benutzeranmeldeinformationen oder ein freigegebenes Zertifikatprofil verwenden muss. Sie können ein Zertifikat mit einer oder mehreren angegebenen Apps oder allen verwalteten Apps verwenden. Sie können auch angeben, ob eine App ein Zertifikat immer dann verwendet, wenn ein Zertifikat erforderlich ist, oder nur für Verbindungen zu einer bestimmten URI.

In einem einzigen Profil können mehrere Zertifikatzuordnungen angegeben werden. Einem Benutzer kann nur ein Zertifikatzuordnungsprofil zugewiesen werden.

Erstellen eines Profils mit Zertifikatzuordnung

Bevor Sie beginnen: Erstellen Sie alle Profile für SCEP, Benutzeranmeldeinformationen oder ein freigegebenes Zertifikat, die zum Senden von Zertifikaten an Geräte und zur Zuordnung der Profile zu Benutzern oder Gruppen erforderlich sind.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf Zertifikate > Zertifikatzuordnung.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
5. Klicken Sie in der Zuordnungstabelle auf +.
6. Wählen Sie unter **Ziel-URI** eine der folgenden Optionen aus:
   - Wählen Sie **Keine** aus, wenn die App das Zertifikat nicht verwendet, um eine Verbindung mit einer Ressource zu authentifizieren.

- Wählen Sie **Alle** aus, wenn die App das Zertifikat verwenden kann, um eine Verbindung mit einer beliebigen Ressource zu authentifizieren.
- Wählen Sie **Angegebener Host:Port** aus und geben Sie den Host und den Port ein, wenn die App das Zertifikat zur Authentifizierung mit einer bestimmten Ressource verwenden kann.

7. Führen Sie unter **App-Zertifikat** eine der folgenden Aktionen durch:
   - Um anzugeben, dass die App ein Zertifikat verwenden muss, das über ein anderes Profil an das Gerät gesendet wird, wählen Sie **Ausgewähltes Zertifikat** und den Profilnamen aus der Dropdown-Liste aus.
   - Um anzugeben, dass die App ein Zertifikat verwenden muss, das von einer Drittanbieterquelle an das Gerät gesendet wurde, wählen Sie **Zertifikatsalias** aus und geben Sie den Alias für das Zertifikat an. Wenn Sie den Alias nicht kennen, beziehen Sie sich auf die Dokumentation oder wenden Sie sich an den Administrator des Zertifikatsanbieters.
   - Um anzugeben, dass die App ein Zertifikat verwenden muss, das über ein anderes Profil an das Gerät gesendet wird, wählen Sie **Ausgewähltes Zertifikat** und den Profilnamen aus der Dropdown-Liste aus.
8. Führen Sie unter **Zugelassene Apps für Ziel-URI** eine der folgenden Aktionen durch:
   - Um jeder verwalteten App zu ermöglichen, das angegebene Zertifikat anzufordern, wählen Sie **Beliebige Apps im geschäftlichen Bereich**.
   - Um nur bestimmten Apps zu ermöglichen, das Zertifikat anzufordern, wählen Sie **Angegebene Apps** und klicken Sie auf +, um eine oder mehrere Apps anzugeben.
9. Wiederholen Sie bei Bedarf die Schritte 5 bis 8, um zusätzliche Zuordnungen zu dem Profil hinzuzufügen.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.
- Legen Sie ggf. eine Rangfolge für die Profile fest.

Verwalten von Clientzertifikaten für Benutzerkonten

Sie können Clientzertifikate direkt zu einzelnen Benutzerkonten oder zu einem Profil für Benutzeranmeldeinformationen hinzufügen, das dem Benutzerkonto zugewiesen ist. Das direkte Hinzufügen von Zertifikaten zu einem Benutzerkonto wird für Geräte, auf denen BlackBerry Dynamics aktiviert ist, oder andere verwaltete iOS- und Android-Geräte unterstützt. Das Hochladen von Zertifikaten zu Profilen mit Anmeldeinformationen wird für Geräte mit BlackBerry 10 OS Version 10.3.1 und höher, iOS-Geräte und Android Enterprise-Geräte unterstützt..

Verwenden Sie ein Profil für Benutzeranmeldeinformationen, das mit einem Wi-Fi-, VPN- oder E-Mail-Profil verknüpft werden kann, und gestatten Sie Benutzern dadurch, Zertifikate hochzuladen und dann zur Verbindung mit Ihrem geschäftlichen Wi-Fi-Netzwerk, VPN und Mailserver zu verwenden.

Wenn Sie über eine lokale Umgebung verfügen und Zertifikate für BlackBerry Dynamics-Apps auf Benutzerkonten hochladen, sollten Sie eine Gültigkeitsdauer für Benutzerzertifikate festlegen. Wenn die Gültigkeitsdauer abgelaufen ist, werden die Zertifikate vom Server gelöscht.

Hinzufügen eines Client-Zertifikats zu einem Benutzerkonto

Sie können einem einzelnen Benutzerkonto ein Client-Zertifikat hinzufügen und dieses Zertifikat an BlackBerry Dynamics-fähige Geräte oder andere verwaltete iOS- und Android-Geräte senden.

Fügen Sie Client-Zertifikate zu Benutzerkonten hinzu, wenn Benutzergeräte Zertifikate für S/MIME oder die Client-Authentifizierung benötigen und das Zertifikat nicht über ein Profil für Benutzeranmeldeinformationen oder ein SCEP-Profil an Geräte gesendet werden kann.

Client-Zertifikate müssen über die Dateierweiterung .pfx oder .p12 verfügen. Sie können mehr als ein Client-Zertifikat an Geräte senden.

Sie können zudem Profile für Benutzeranmeldeinformationen verwenden, um Zertifikate für einzelne Benutzer hochzuladen. Profile für Benutzeranmeldeinformationen können mit einem Wi-Fi-, VPN- oder E-Mail-Profil verknüpft werden.

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 eines Benutzerkontos.
4. Klicken Sie im Abschnitt **IT-Richtlinien und -Profile** auf +.
5. Klicken Sie auf **Benutzerzertifikat**.
6. Geben Sie eine Beschreibung für das Zertifikat ein.
7. Wählen Sie im Abschnitt **Zertifikat anwenden auf** eine der folgenden Optionen aus:
   - **Andere verwaltete Geräte**: Wählen Sie diese Option aus, um das Zertifikat an iOS- und Android-Geräte für alle anderen unterstützten Nutzungszwecke außer für BlackBerry Dynamics-Apps zu senden.
   - **BlackBerry Dynamics-fähige Geräte**: Wählen Sie diese Option aus, um das Zertifikat zur Verwendung mit BlackBerry Dynamics-Apps an Geräte zu senden.
8. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
9. Wenn Sie **Andere verwaltete Geräte** aktiviert haben, geben Sie ein Kennwort für das Zertifikat in das Feld **Kennwort** ein. Für iOS-Geräte ist ein Kennwort erforderlich. Für Android-Geräte muss kein Kennwort in BlackBerry UEM festgelegt werden, wenn auf dem Gerät die aktuelle Version von BlackBerry UEM Client ausgeführt wird. Wenn Sie kein Kennwort festlegen, muss der Benutzer das Gerätekennwort eingeben.
10. Klicken Sie auf **Hinzufügen**.
    Das Zertifikat wird in der Tabelle **Benutzerzertifikate** auf der Seite „Zusammenfassung“ aufgeführt.

Wenn Sie fertig sind:

- Konfigurieren Sie für BlackBerry Dynamics-fähige Geräte die Zeitspanne, über die hochgeladene Zertifikate auf dem BlackBerry UEM Server verbleiben, bevor sie automatisch vom Server gelöscht werden. Der Standardwert ist 24 Stunden.

Hinzufügen eines Client-Zertifikats für ein Benutzerkonto

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 eines Benutzerkontos.
4. Klicken Sie im Abschnitt **IT-Richtlinie und Profile** auf das zu ändernde Benutzerzertifikat.
5. Klicken Sie auf .
6. Nehmen Sie die notwendigen Änderungen vor. Sie können nicht ändern, zu welchen Geräten das Zertifikat gehört.
7. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Wenn Sie ein BlackBerry Dynamics-Benutzerzertifikat ändern, das von Ihnen oder von einem Benutzer von einem Gerät entfernt wurde, wird das Zertifikat erneut an das Gerät gesendet.

Hinzufügen eines Client-Zertifikats zu einem Profil mit Benutzeranmeldeinformationen

Sie können Zertifikate für einzelne Benutzer in ein Profil mit Benutzeranmeldeinformationen hochladen. Benutzer können ihre Zertifikate zudem mithilfe von BlackBerry UEM Self-Service in das entsprechende Profil hochladen. Das Hochladen von Zertifikaten zu Profilen mit Anmeldeinformationen wird für Geräte mit BlackBerry 10 OS Version 10.3.1 und höher, iOS-Geräte und Android Enterprise-Geräte unterstützt.

Client-Zertifikate müssen über die Dateierweiterung .pfx oder .p12 verfügen. Wenn Sie oder ein Benutzer ein neues Zertifikat in ein Profil mit Benutzeranmeldeinformationen hochlädt, ersetzt es das vorhandene Zertifikat auf den Benutzergeräten.

Bevor Sie beginnen:

- Profil mit Benutzeranmeldeinformationen zum manuellen Hochladen von Zertifikaten erstellen.
- Weisen Sie Benutzern das Profil mit Anmeldeinformationen zu.

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 eines Benutzerkontos.
4. Klicken Sie im Abschnitt **IT-Richtlinie und -Profile** neben dem Profil für Benutzeranmeldeinformationen auf **Ein Zertifikat hinzufügen**.
5. Klicken Sie auf **Durchsuchen**, um zum Speicherort der Zertifikatdatei zu navigieren.
6. Geben Sie das Kennwort für das Zertifikat ein. Für iOS-Geräte ist das Kennwort erforderlich. Für Android-Geräte muss das Kennwort in BlackBerry UEM nicht angegeben werden, wenn auf dem Gerät die aktuelle Version von BlackBerry UEM Client ausgeführt wird. Wenn Sie das Kennwort nicht festlegen, muss der Benutzer das Gerätekennwort eingeben.
7. Klicken Sie auf **Hinzufügen**.

Hinzufügen eines Client-Zertifikats für ein Profil mit Benutzeranmeldeinformationen

Sie können das von Ihnen oder einem Benutzer zu einem Profil mit Anmeldeinformationen hinzugefügte Zertifikat ändern. Das neue Zertifikat ersetzt das auf dem Gerät vorhandene Zertifikat.

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 eines Benutzerkontos.
4. Klicken Sie im Abschnitt **IT-Richtlinie und Profile** in der Zeile für das Profil mit Benutzeranmeldeinformationen auf **Aktualisieren**.
5. Klicken Sie auf **Durchsuchen**, um zum Speicherort der Zertifikatdatei zu navigieren.
6. Geben Sie ein Kennwort für das Zertifikat ein. Für iOS-Geräte ist ein Kennwort erforderlich. Für Android-Geräte muss das Kennwort in BlackBerry UEM nicht angegeben werden, wenn auf dem Gerät die aktuelle Version von BlackBerry UEM Client ausgeführt wird. Wenn Sie das Kennwort nicht festlegen, muss der Benutzer das Gerätekennwort eingeben.
7. Klicken Sie auf **Speichern**.

Konfigurieren der Gültigkeitsdauer für Clientzertifikate

Wenn Sie Zertifikate für BlackBerry Dynamics-Apps auf einzelne Benutzerkonten hochladen, sollten Sie eine Gültigkeitsdauer für Clientzertifikate festlegen. Wenn die Gültigkeitsdauer abgelaufen ist, werden die Zertifikate vom Server gelöscht. Damit wird verhindert, dass ein Clientzertifikat eine längere Zeit auf dem Server verbleibt, nachdem die Push-Übertragung auf das Gerät erfolgt ist. Die standardmäßige Gültigkeitsdauer liegt bei 24 Stunden.

Diese Funktion wird in BlackBerry UEM Cloud nicht unterstützt.

1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Zertifikate**.
2. Legen Sie die Gültigkeitsdauer für PKCS12-Zertifikate auf dem Server fest.

Wenn Sie fertig sind: Wenn noch nicht erfolgt, fügen Sie den Benutzerkonten Clientzertifikate hinzu.

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