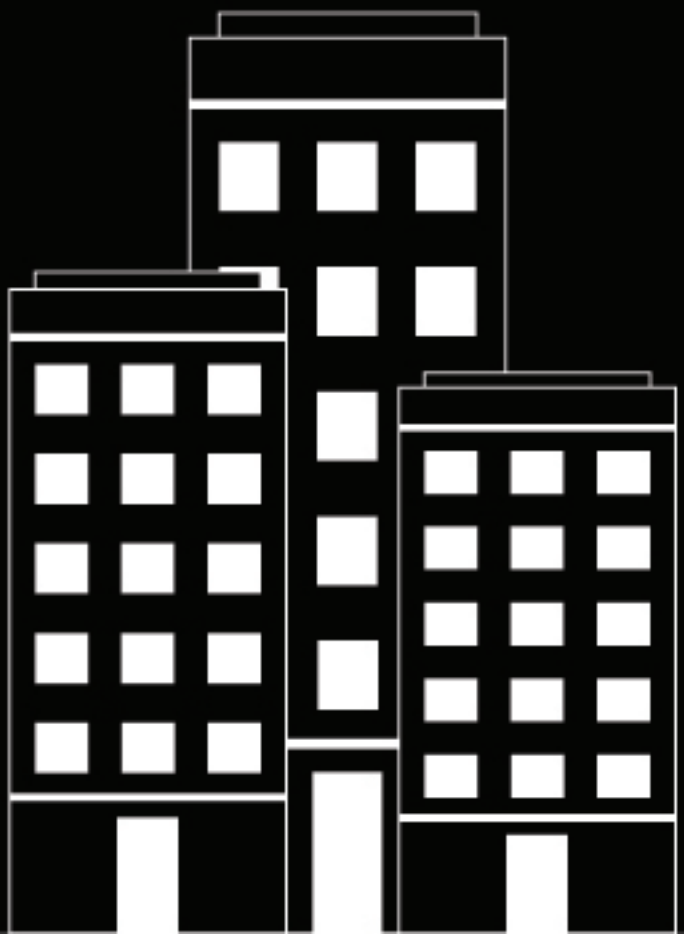

BlackBerry UEM

Sichere Verbindungen verwalten

12.20

Contents

Verwalten sicherer Verbindungen mit BlackBerry UEM.....5

Verwalten von geschäftlichen Verbindungen mithilfe von Profilen..... 7

Einrichten von geschäftlichen Wi-Fi-Netzwerken für Geräte.....7
Erstellen eines Wi-Fi-Profils.....7
iOS und macOS: Wi-Fi-Profileinstellungen..... 8
Android: Wi-Fi-Profileinstellungen.....13
Windows: Wi-Fi-Profileinstellungen..... 16
Einrichten von geschäftlichen VPNs für Geräte..... 20
Erstellen eines VPN-Profils..... 21
iOS und macOS: VPN-Profileinstellungen..... 22
Android: VPN-Profileinstellungen.....32
Windows 10: VPN-Profileinstellungen.....36
Integration von BlackBerry UEM in CylanceGATEWAY zum Erstellen eines ZTNA-Profils..... 40
Aktivieren und Zuweisen von Per-App-VPN-Einstellungen.....41
Einrichten von Proxy-Profilen für Geräte..... 42
Erstellen eines Proxy-Profils..... 43
Verwenden von BlackBerry Secure Connect Plus für Verbindungen mit geschäftlichen Ressourcen..... 44
Server- und Geräteanforderungen für BlackBerry Secure Connect Plus.....45
Enable BlackBerry Secure Connect Plus.....47
Aktualisieren der BlackBerry Connectivity-App.....48
Aktualisieren der BlackBerry Connectivity-App für Samsung Knox Workspace- und Android Enterprise-Geräte, die keinen Zugriff auf Google Play haben..... 48
Enterprise-Konnektivitätsprofileinstellungen.....49
Festlegen der DNS-Einstellungen für die BlackBerry Connectivity-App..... 52
Optimieren von sicheren Tunnelverbindungen für Android-Geräte, die BlackBerry Dynamics-Apps verwenden..... 52
Fehlerbehebung für BlackBerry Secure Connect Plus..... 53
Verwenden von BlackBerry 2FA für sichere Verbindungen mit kritischen Ressourcen..... 54
Aktivieren der automatischen Authentifizierung für iOS-Geräte.....55
Angeben des DNS-Servers für iOS- und macOS-Geräte.....56
Angeben von E-Mail- und Webdomänen für iOS-Geräte..... 57
Kontrollieren der Netzwerknutzung von Apps auf iOS-Geräten.....58
Erstellen von Webinhaltsfilter-Profilen auf iOS-Geräten.....58
Erstellen eines AirPrint-Profils für iOS-Geräte.....60
Erstellen eines AirPlay-Profils für iOS-Geräte..... 61
Erstellen eines APN-Profils für Android-Geräte..... 61
Einstellungen für APN-Profil..... 62

Verwenden von PKI-Zertifikaten mit Geräten oder Apps.....64

Vernetzung von BlackBerry UEM und der PKI-Software Ihrer Organisation..... 65
Herstellen einer Verbindung zwischen BlackBerry UEM und der Entrust-Software Ihres Unternehmens..... 65
Verbinden von BlackBerry UEM mit dem Entrust IdentityGuard-Server Ihres Unternehmens mit Smart Credentials..... 66

Herstellen einer Verbindung zwischen BlackBerry UEM und der OpenTrust-Software Ihres Unternehmens.....66
Verbindung von BlackBerry UEM mit einer BlackBerry Dynamics-PKI-Verbindung.....67
Herstellen einer Verbindung zwischen BlackBerry UEM und der App-basierten PKI-Lösung Ihrer Organisation.....68
Bereitstellen von Clientzertifikaten für Geräte und Apps.....68
Senden von Clientzertifikaten an Geräte und Apps mithilfe von Profilen.....70
Senden von Zertifizierungsstellenzertifikaten an Geräte und Apps.....71
Senden von Clientzertifikaten an Geräte und Apps unter Verwendung von Profilen für Benutzeranmeldeinformationen.....72
Erstellen eines Profils für Benutzeranmeldeinformationen zur Verbindung mit Ihrer BlackBerry Dynamics-PKI-Software.....76
Senden von Clientzertifikaten an Geräte und Apps mithilfe von SCEP.....81
Senden des gleichen Clientzertifikats an mehrere Geräte.....90
Angeben des Zertifikats, das von einer App mit einem Zertifikatzuordnungsprofil verwendet wird.....90
Verwalten von Clientzertifikaten für Benutzerkonten.....92
Hinzufügen und Verwalten eines Client-Zertifikats für ein Benutzerkonto.....92

Rechtliche Hinweise.....96

Verwalten sicherer Verbindungen mit BlackBerry UEM

In der folgenden Tabelle sind die Verwaltungsaufgaben zusammengefasst, die in dieser Anleitung besprochen werden. Überprüfen Sie, welche Aufgaben Sie gemäß den Anforderungen Ihres Unternehmens erledigen sollten.

Aufgabe	Beschreibung
Erstellen eines WLAN-Profils	Sie können ein Wi-Fi-Profil erstellen, um festzulegen, wie Geräte eine Verbindung zu geschäftlichen Wi-Fi-Netzwerken herstellen.
Erstellen eines VPN-Profils	Sie können ein VPN-Profil erstellen, um festzulegen, wie Geräte eine Verbindung zu einem geschäftlichen VPN aufbauen.
Erstellen eines Per-App-VPN-Profils	Sie können angeben, welche Apps auf den Geräten ein VPN für die Datenübertragung verwenden müssen.
Erstellen eines Proxy-Profils	Sie können festlegen, wie die Geräte einen Proxy-Server nutzen, um auf Webdienste im Internet oder auf ein geschäftliches Netzwerk zuzugreifen.
Erstellen eines Enterprise-Konnektivitätsprofils	Sie können festlegen, wie Geräte über Enterprise-Konnektivität und BlackBerry Secure Connect Plus mit den Ressourcen Ihres Unternehmens verbunden werden, um einen sicheren IP-Tunnel zwischen Apps und dem Netzwerk Ihres Unternehmens bereitzustellen.
Erstellen eines BlackBerry 2FA-Profils	Sie können den Einsatz der Zwei-Faktor-Authentifizierung für Benutzer ermöglichen und die Konfiguration der Funktionen für Vorauthentifizierung und Wiederherstellung festlegen.
SSO-Erweiterungsprofil erstellen	Sie können iOS und iPadOS-Geräten ermöglichen, sich bei Domänen und Webdiensten Ihres Unternehmensnetzwerks automatisch zu authentifizieren.
Erstellen eines BlackBerry Dynamics-Konnektivitätsprofils	Sie können die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server festlegen, mit denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können. Weitere Informationen finden Sie unter Einrichten von Netzwerkverbindungen für BlackBerry Dynamics-Apps in der Dokumentation für Administratoren.
Erstellen eines DNS-Profils	Sie können die DNS-Server angeben, die iOS- und macOS-Geräte für den Zugriff auf bestimmte Domänen verwenden sollen.
Erstellen eines E-Mail-Profils	Sie können festlegen, wie Geräte eine Verbindung zum geschäftlichen E-Mail-Server herstellen und E-Mail-Nachrichten und Kalendereinträge mithilfe von Exchange ActiveSync oder IBM Notes Traveler synchronisieren. Weitere Informationen finden Sie unter Erstellen von E-Mail-Profilen in der Dokumentation für Administratoren.
Erstellen eines IMAP/POP3-E-Mail-Profils	Sie können festlegen, wie Geräte eine Verbindung mit einem IMAP- bzw. POP3-E-Mail-Server aufbauen und E-Mail-Nachrichten synchronisieren. Weitere Informationen finden Sie unter Erstellen eines IMAP/POP3-E-Mail-Profils in der Dokumentation für Administratoren.

Aufgabe	Beschreibung
Erstellen eines Netzwerknutzungsprofils	Sie können die Nutzung des mobilen Netzwerks für iOS- und iPadOS-Apps verwalten.
Erstellen von Webinhaltsfilter-Profilen	Sie können die Websites einschränken, die ein Benutzer in Safari oder in anderen Browsern auf einem iOS- oder iPadOS-Gerät unter Aufsicht aufrufen kann.
Erstellen eines AirPrint-Profils	Sie können Benutzern dabei helfen, Drucker zu finden.
Erstellen eines AirPlay-Profils	Sie können festlegen, zu welchen AirPlay-Geräten Benutzer von iOS und iPadOS eine Verbindung herstellen können.
Erstellen eines APN-Profils	Sie können die Informationen angeben, die Android-Geräte brauchen, um mit dem Netzwerk des Anbieters zu kommunizieren.
Verbinden von UEM mit der PKI-Software Ihres Unternehmens	Sie können die zertifikatbasierte Authentifizierung, die von Ihren PKI-Diensten bereitgestellt wird, auf die Geräte und Apps erweitern, die Sie mit UEM verwalten. Sie können beispielsweise Folgendes tun • Herstellen einer Verbindung zwischen BlackBerry UEM und der Entrust-Software Ihres Unternehmens • Verbinden von BlackBerry UEM mit dem Entrust IdentityGuard-Server Ihres Unternehmens mit Smart Credentials • Herstellen einer Verbindung zwischen BlackBerry UEM und der OpenTrust-Software Ihres Unternehmens • Verbindung von BlackBerry UEM mit einer BlackBerry Dynamics-PKI-Verbindung • Herstellen einer Verbindung zwischen BlackBerry UEM und der App-basierten PKI-Lösung Ihrer Organisation
Senden von Zertifikaten an Geräte und Apps mithilfe von Profilen	Sie können Zertifikate an Geräte und Apps mithilfe von UEM-Profilen senden.
Verwalten von Clientzertifikaten für Benutzerkonten	Sie können Clientzertifikate direkt zu einzelnen Benutzerkonten oder zu einem Profil für Benutzeranmeldeinformationen hinzufügen, das dem Benutzerkonto zugewiesen ist.

Verwalten von geschäftlichen Verbindungen mithilfe von Profilen

Sie können Profile verwenden, um Geschäftsverbindungen für Geräte in Ihrer Organisation einzurichten und zu verwalten. Geschäftsverbindungen legen fest, wie die Geräte eine Verbindung zu den geschäftlichen Ressourcen in Ihrem Unternehmensnetzwerk aufbauen, z. B. zu Mailservern, Proxy-Servern, Wi-Fi-Netzwerken und VPNs. Sie können Einstellungen für iOS-, macOS-, Android- und Windows 10-Geräte in dem gleichen Profil festlegen und das Profil dann Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen.

Einige Geschäftsverbindungsprofile können ein oder mehrere verknüpfte Profile enthalten. Wenn Sie ein angeschlossenes Profil festlegen, verknüpfen Sie ein vorhandenes Profil mit einem Geschäftsverbindungsprofil, und die Geräte müssen das angeschlossene Profil verwenden, wenn sie das Verbindungsprofil nutzen. Sie können beispielsweise Zertifikatsprofile und Proxyprofile diversen Profilen für geschäftliche Verbindungen zuweisen. Profile müssen in der folgenden Reihenfolge erstellt werden:

1. Zertifikatsprofile
2. Proxy-Profile
3. Profile für geschäftliche Verbindungen, z. B. E-Mail, VPN und Wi-Fi

Wenn Sie beispielsweise zuerst ein Wi-Fi-Profil erstellen, können Sie bei der Erstellung eines Proxy-Profils dieses nicht mit dem Wi-Fi-Profil verknüpfen. Nach dem Erstellen eines Proxy-Profils müssen Sie das Wi-Fi-Profil ändern, um es mit dem Proxy-Profil verknüpfen zu können.

Einrichten von geschäftlichen Wi-Fi-Netzwerken für Geräte

Sie können Wi-Fi-Profile verwenden, um festzulegen, wie Geräte eine Verbindung zu geschäftlichen Wi-Fi-Netzwerken hinter der Firewall herstellen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Wi-Fi-Profil zuweisen.

Standardmäßig können sowohl geschäftliche als auch persönliche Apps Wi-Fi-Profile verwenden, um eine Verbindung zum Netzwerk Ihres Unternehmens herzustellen.

Erstellen eines Wi-Fi-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen vom Wi-Fi-Sicherheitstyp und dem Authentifizierungsprotokoll ab, die Sie ausgewählt haben. Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben.

Bevor Sie beginnen:

- Wenn die Geräte eine zertifikatbasierte Authentifizierung für Wi-Fi-Geschäftsverbindungen verwenden, erstellen Sie ein Profil mit Zertifizierungsstellenzertifikat, und weisen Sie es Benutzerkonten, Benutzergruppen oder Gerätegruppen zu. Um Clientzertifikate an Geräte zu senden, erstellen Sie ein SCEP-Profil, ein Profil für ein freigegebenes Zertifikat oder ein Profil für Benutzeranmeldeinformationen, das Sie mit dem Wi-Fi-Profil verknüpfen.
- Bei iOS-, iPadOS-, macOS- und Android Enterprise-Geräten, die einen Proxy-Server für geschäftliche Wi-Fi-Verbindungen verwenden, müssen Sie ein Proxy-Profil erstellen, das mit dem Wi-Fi-Profil verknüpft werden soll.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > WLAN**.
3. Klicken Sie auf +.

4. Geben Sie einen Namen und eine Beschreibung für das Wi-Fi-Profil ein. Diese Informationen werden auf den Geräten angezeigt.
5. Geben Sie im Feld **SSID** den Netzwerknamen eines Wi-Fi-Netzwerks ein.
6. Wenn das Wi-Fi-Netzwerk die SSID nicht sendet, aktivieren Sie das Kontrollkästchen **Verborgenes Netzwerk**.
7. Klicken Sie auf die Registerkarte für einen Gerätetyp, um die zutreffenden Einstellungen zu konfigurieren. Weitere Informationen finden Sie in den Wi-Fi-Profileinstellungen für iOS und macOS, Android und Windows.

   Wenn Ihr Unternehmen erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für den Zugriff auf das Wi-Fi-Netzwerk eingeben, geben Sie `%UserName%` im Feld **Benutzername** ein.
8. Wiederholen Sie Schritt 7 für jeden Gerätetyp.
9. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Wi-Fi-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

iOS und macOS: Wi-Fi-Profileinstellungen

iOS, iPadOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Profil anwenden auf	Diese Einstellung gibt an, ob das Wi-Fi-Profil auf einem macOS-Gerät für das Benutzerkonto oder das Gerät gilt.
Automatisch dem Netzwerk beitreten	Diese Einstellung gibt an, ob ein Gerät dem Wi-Fi-Netzwerk automatisch hinzugefügt werden kann.
MAC-Randomisierung deaktivieren	Diese Einstellung legt fest, ob Geräte ihre MAC-Adressen zufällig zuweisen können, wenn sie eine Verbindung zum Wi-Fi-Netzwerk herstellen.
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.
Netzwerktyp	Diese Einstellung legt eine Konfiguration für das Wi-Fi-Netzwerk fest. Hotspot-Konfigurationen stehen nur für iOS-, iPadOS- und macOS-Geräte zur Verfügung. Wenn Sie eine der Hotspot-Optionen auswählen, verwenden Sie nicht dasselbe Wi-Fi-Profil, um Einstellungen für andere Gerätetypen zu konfigurieren.
Angezeigter Betreibername	Diese Einstellung legt den Anzeigenamen des Hotspot-Betreibers fest. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Domänenname	Diese Einstellung legt den Domänennamen des Hotspot-Betreibers fest. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist. Wenn Sie diese Einstellung verwenden, ist die Einstellung „SSID“ nicht erforderlich.
Unternehmensbezeichner der Roaming-Konsortien	Diese Einstellung legt die Organisationsbezeichner der Roaming-Konsortien und Dienstanbieter fest, auf die über den Hotspot zugegriffen werden kann. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.

iOS, iPadOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
NAI-Bereichsnamen	Diese Einstellung legt die NAI-Bereichsnamen fest, die ein Gerät authentifizieren können. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
MCC/MNCs	Diese Einstellung legt die MCC/MNC-Kombinationen fest, die Mobilfunknetzbetreiber identifizieren. Jeder Wert muss genau sechs Ziffern umfassen. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Verbindungsaufbau zu Roaming-Partnernetzwerken zulassen	Diese Einstellung legt fest, ob ein Gerät eine Verbindung zu Roaming-Partnern für den Hotspot aufbauen kann. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Wenn die Einstellung „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist, ist diese Einstellung auf „WPA2-Enterprise“ gesetzt.
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“, „WPA2-Personal“ oder „WPA3-Personal“ gesetzt ist.
Protokolle	
Authentifizierungsprotokoll	Diese Einstellung legt die EAP-Methoden fest, die das Wi-Fi-Netzwerk unterstützt. Sie können mehrere EAP-Methoden auswählen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Interne Authentifizierung	Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist.

iOS, iPadOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
PAC verwenden	Diese Einstellung legt fest, ob die EAP-FAST-Methode geschützte Anmeldeinformationen (Protected Access Credential) verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist.
PAC bereitstellen	Diese Einstellung legt fest, ob die EAP-FAST-Methode die Bereitstellung von geschützten Anmeldeinformationen zulässt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt und die Einstellung „PAC verwenden“ ausgewählt ist.
PAC anonym bereitstellen	Diese Einstellung legt fest, ob die EAP-FAST-Methode die anonyme Bereitstellung von geschützten Anmeldeinformationen zulässt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist und die Einstellungen „PAC verwenden“ und „PAC bereitstellen“ ausgewählt sind.
Authentifizierung	
Externe Identität für TTLS, PEAP und EAP-FAST	Diese Einstellung legt die externe Identität für einen Benutzer fest, die als Klartext gesendet wird. Sie können einen anonymen Benutzernamen festlegen, um die echte Identität des Benutzers zu verbergen (beispielsweise „anonym“). Der verschlüsselte Tunnel wird verwendet, um den echten Benutzernamen zur Authentifizierung beim Wi-Fi-Netzwerk zu senden. Wenn die externe Identität den Bereichsnamen enthält, um die Anforderung weiterzuleiten, muss es sich dabei um den tatsächlichen Bereich des Benutzers handeln (beispielsweise „anonym@Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“, „PEAP“ oder „EAP-FAST“ gesetzt ist.
Im Wi-Fi-Profil enthaltenes Kennwort verwenden	Diese Einstellung legt fest, ob das Wi-Fi-Profil das Kennwort für die Authentifizierung enthält. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, das ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Im Wi-Fi-Profil enthaltenes Kennwort verwenden“ ausgewählt wurde.

iOS, iPadOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Gerät verwendet, um eine Verbindung zum Wi-Fi-Netzwerk aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für das mit dem Wi-Fi-Profil verknüpfte Client-Zertifikat fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Profil für freigegebenes Zertifikat	Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Clientzertifikat fest, das ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Name des Clientzertifikats	Diese Einstellung legt den Namen des Clientzertifikats fest, das ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
Vertrauen	

iOS, iPadOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Profile für Zertifizierungsstellenzertifikate	Diese Einstellung legt die Profile für Zertifizierungsstellenzertifikate mit den vertrauenswürdigen Zertifikaten fest, die ein Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Vertrauenswürdige Zertifikatnamen	Diese Einstellung legt die Namen der vertrauenswürdigen Zertifikate fest, die ein Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.
Benutzerentscheidungen vertrauen	Diese Einstellung legt fest, ob ein Gerät den Benutzer auffordert, einem Server zu vertrauen, wenn die Vertrauenskette nicht hergestellt werden kann. Wenn diese Einstellung nicht ausgewählt ist, können nur Verbindungen zu von Ihnen festgelegten vertrauenswürdigen Servern aufgebaut werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Captive-Netzwerk umgehen	Diese Einstellung legt fest, ob Geräte Captive-Netzwerke umgehen können.
QoS-Markierung aktivieren	Diese Einstellung legt fest, ob Sie eine L2- oder L3-Markierung für Datenverkehr über das Wi-Fi-Netzwerk aktivieren können.
QoS für FaceTime-Anrufe verwenden	Diese Einstellung legt fest, ob Audio- und Videodatenverkehr für FaceTime-Anrufe L2- und L3-Markierungen verwenden kann.
Nur L2-Markierung für den QoS-Datenverkehr verwenden	Diese Einstellung legt fest, ob Datenverkehr über das Wi-Fi-Netzwerk nur die L2-Markierung verwendet.
QoS-Markierung auf ausgewählte Apps anwenden	Diese Einstellung legt die Bundle-IDs für Apps fest, die die L2- und L3-Markierung verwenden können.

Android: Wi-Fi-Profileinstellungen

Android: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, mit dem Android-Geräte die Verbindung zu einem Proxy-Server herstellen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist. Auf Geräten mit Android, die über MDM-Steuerelemente- oder Privatsphäre des Benutzers-Aktivierungen verfügen, werden Wi-Fi-Profile mit Proxyeinstellungen nicht unterstützt.
BSSID	Diese Einstellung legt die MAC-Adresse eines drahtlosen Zugriffspunkts im Wi-Fi-Netzwerk fest.
Primärer DNS	Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung gilt nur für Geräte, die Samsung Knox verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.
Sekundärer DNS	Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung gilt nur für Geräte, die Samsung Knox verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet.
Persönlicher Sicherheitstyp	Diese Einstellung legt den persönlichen Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Persönlich“ gesetzt ist.
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WPA-Personal/WPA2-Personal“ gesetzt ist.

Android: Wi-Fi-Profileinstellung	Beschreibung
Authentifizierungsprotokoll	Diese Einstellung legt die EAP-Methode fest, die das Wi-Fi-Netzwerk verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist. LEAP wird von Geräten, die Samsung Knox verwenden, nicht unterstützt.
Interne Authentifizierung	Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist. CHAP wird von Geräten, die Samsung Knox verwenden, nicht unterstützt.
Externe Identität für TTLS	Diese Einstellung legt die externe Identität für einen Benutzer fest, die als Klartext gesendet wird. Sie können einen anonymen Benutzernamen festlegen, um die echte Identität des Benutzers zu verbergen (beispielsweise „anonym“). Der verschlüsselte Tunnel wird verwendet, um den echten Benutzernamen zur Authentifizierung beim Wi-Fi-Netzwerk zu senden. Wenn die externe Identität den Bereichsnamen enthält, um die Anforderung weiterzuleiten, muss es sich dabei um den tatsächlichen Bereich des Benutzers handeln (beispielsweise „anonym@Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist.
Externe Identität für PEAP	Diese Einstellung legt die externe Identität für einen Benutzer fest, die als Klartext gesendet wird. Sie können einen anonymen Benutzernamen festlegen, um die echte Identität des Benutzers zu verbergen (beispielsweise „anonym“). Der verschlüsselte Tunnel wird verwendet, um den echten Benutzernamen zur Authentifizierung beim Wi-Fi-Netzwerk zu senden. Wenn die externe Identität den Bereichsnamen enthält, um die Anforderung weiterzuleiten, muss es sich dabei um den tatsächlichen Bereich des Benutzers handeln (beispielsweise „anonym@Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“ gesetzt ist.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Im Wi-Fi-Profil enthaltenes Kennwort verwenden	Diese Einstellung legt fest, ob das Wi-Fi-Profil das Kennwort für die Authentifizierung enthält. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.

Android: Wi-Fi-Profileinstellung	Beschreibung
Kennwort	Diese Einstellung legt das Kennwort fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Im Wi-Fi-Profil enthaltenes Kennwort verwenden“ ausgewählt wurde.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Android-Gerät verwendet, um eine Verbindung zum Wi-Fi-Netzwerk aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für das mit dem Wi-Fi-Profil verknüpfte Client-Zertifikat fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Profil für freigegebenes Zertifikat	Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Clientzertifikat fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist. Der Name des Profils für das freigegebene Zertifikat muss für Geräte, die einen Knox Workspace verwenden, weniger als 36 Zeichen enthalten.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Android-Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist. Der Name des SCEP-Profils muss für Geräte, die einen Knox Workspace verwenden, weniger als 36 Zeichen enthalten.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Android-Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist. Der Name des Profils für Benutzeranmeldeinformationen muss für Geräte, die einen Knox Workspace verwenden, weniger als 36 Zeichen enthalten.
Name des Clientzertifikats	Diese Einstellung legt den Namen des Clientzertifikats fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.

Android: Wi-Fi-Profileinstellung	Beschreibung
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Zertifizierungsstellenzertifil Profil	Diese Einstellung legt das Profil mit Zertifizierungsstellenzertifikat mit dem vertrauenswürdigen Zertifikat fest, die ein Android-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Vertrauenswürdige Zertifikatnamen	Diese Einstellung legt die Namen der vertrauenswürdigen Zertifikate fest, die ein Android-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.

Windows: Wi-Fi-Profileinstellungen

Windows: Wi-Fi-Profileinstellung	Beschreibung
Automatisch verbinden, wenn das Netzwerk in Reichweite ist	Diese Einstellung gibt an, ob Geräte automatisch eine Verbindung mit dem Wi-Fi-Netzwerk herstellen können.
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet.
Verschlüsselungstyp	Diese Einstellung legt die Verschlüsselungsmethode fest, die das Wi-Fi-Netzwerk verwendet. Die Einstellung „Sicherheitstyp“ legt fest, welche Verschlüsselungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird.

Windows: Wi-Fi-Profileinstellung	Beschreibung
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Offen“ und der „Verschlüsselungstyp“ auf „WEP“ gesetzt ist.
Schlüsselindex	Diese Einstellung legt die Position des entsprechenden, auf dem drahtlosen Zugriffspunkt gespeicherten Schlüssels fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Offen“ und der „Verschlüsselungstyp“ auf „WEP“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ gesetzt ist.
Single Sign-On aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die Authentifizierung nach einmaliger Anmeldung unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.
Typ der einmaligen Anmeldung	Diese Einstellung legt fest, wann die Authentifizierung nach einmaliger Anmeldung durchgeführt wird. Wenn diese Einstellung auf „Direkt vor Benutzeranmeldung durchführen“ gesetzt ist, wird die einmalige Anmeldung durchgeführt, bevor sich der Benutzer bei Active Directory anmeldet. Wenn diese Einstellung auf „Direkt nach Benutzeranmeldung durchführen“ gesetzt ist, wird die einmalige Anmeldung sofort durchgeführt, nachdem sich der Benutzer bei Active Directory angemeldet hat. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.
Maximale Verzögerung für Konnektivität	Diese Einstellung legt fest, wie viele Sekunden verstreichen sollen, bevor der Versuch, die Verbindung durch eine einmalige Anmeldung aufzubauen, fehlschlägt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.

Windows: Wi-Fi-Profileinstellung	Beschreibung
Zulassen, dass weitere Dialoge während der einmaligen Anmeldung angezeigt werden.	Diese Einstellung legt fest, ob ein Gerät außer dem Anmeldebildschirm Dialogfelder anzeigen kann. Wenn es beispielsweise für einen EAP-Authentifizierungstyp erforderlich ist, dass der Benutzer das im Authentifizierungsvorgang vom Server gesendete Zertifikat bestätigt, kann das Gerät das entsprechende Dialogfeld anzeigen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.
Dieses Netzwerk verwendet separate virtuelle LANs für Geräte- und Benutzerauthentifizierung	Diese Einstellung legt fest, ob von den Anmeldeinformationen des Benutzers abhängt, welches VLAN von einem Gerät verwendet wird. Wenn das Gerät beispielsweise beim Starten in ein VLAN platziert wird und dann (auf Grundlage von Benutzerberechtigungen) nach der Anmeldung des Benutzers in ein anderes VLAN-Netzwerk übergeht. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.
Serverzertifikat bewerten	Diese Einstellung legt fest, ob ein Gerät das Serverzertifikat bewerten muss, das die Identität des drahtlosen Zugriffspunkts überprüft. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.
Benutzer nicht auffordern, neue Server oder vertrauenswürdige Zertifizierungsstellen zu autorisieren	Diese Einstellung legt fest, ob ein Benutzer aufgefordert wird, dem Serverzertifikat zu vertrauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Serverzertifikat bewerten“ ausgewählt wurde.
Profile für Zertifizierungsstellenzertifi	Diese Einstellung legt das Profil des Zertifizierungsstellenzertifikats fest, das den Vertrauensstamm für das vom drahtlosen Zugriffspunkt verwendete Serverzertifikat bereitstellt. Diese Einstellung begrenzt die Stammzertifizierungsstellen, denen Geräte vertrauen, auf die ausgewählten Zertifizierungsstellen. Wenn Sie keine vertrauenswürdigen Stammzertifizierungsstellen auswählen, vertrauen die Geräte allen Stammzertifizierungsstellen, die in ihrem Speicher für vertrauenswürdige Stammzertifizierungsstellen aufgelistet sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Serverzertifikat bewerten“ ausgewählt wurde.
Schnelle Wiederherstellung der Verbindung aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die schnelle Wiederherstellung bei PEAP-Authentifizierung über mehrere drahtlose Zugriffspunkte unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.

Windows: Wi-Fi-Profileinstellung	Beschreibung
NAP erzwingen	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk anhand von NAP Systemintegritätsprüfungen auf Geräten durchführen soll, um zu überprüfen, ob die Geräte den Integritätsanforderungen entsprechen, bevor der Verbindungsaufbau zum Netzwerk zugelassen wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.
FIPS-Modus aktivieren	Diese Einstellung gibt an, ob das Wi-Fi-Netzwerk mit dem FIPS 140-2-Standard konform ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA2-Enterprise“ oder „WPA2-Personal“ und der „Verschlüsselungstyp“ auf „WEP“ festgelegt sind.
PMK-Zwischenspeicherung aktivieren	Diese Einstellung legt fest, ob ein Gerät den PMK zwischenspeichern kann, um ein schnelles WPA2 Roaming einzuschalten. Ein schnelles Roaming überspringt 802.1X-Einstellungen mit einem drahtlosen Zugriffspunkt, bei dem sich das Gerät zuvor authentifiziert hat. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA2-Enterprise“ gesetzt ist.
PMK-Lebenszeit	Diese Einstellung legt fest, wie viele Minuten ein Gerät den PMK im Cache speichern kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde.
Anzahl der Einträge im PMK-Cache	Diese Einstellung legt die maximale Anzahl an PMK-Einträgen fest, die ein Gerät im Cache speichern kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde.
Dieses Netzwerk arbeitet mit Vorauthentifizierung	Diese Einstellung legt fest, ob der Zugriffspunkt die Vorauthentifizierung für ein schnelles WPA2 Roaming unterstützt. Vorauthentifizierung ermöglicht Geräten, die eine Verbindung zu einem drahtlosen Zugriffspunkt aufbauen, 802.1X-Einstellungen mit anderen drahtlosen Zugriffspunkten innerhalb seines Bereichs durchzuführen. Bei einer Vorauthentifizierung werden der PMK und die mit ihm verknüpften Informationen im PMK-Cache gespeichert. Wenn das Gerät eine Verbindung zu einem drahtlosen Zugriffspunkt aufbaut, bei dem es sich vorauthentifiziert hat, verwendet es die zwischengespeicherten PMK-Daten, um die Zeit für die Authentifizierung und den Verbindungsaufbau zu verkürzen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde.

Windows: Wi-Fi-Profileinstellung	Beschreibung
Maximale Anzahl der Vorauthentifizierungsversu	Diese Einstellung legt die maximale Anzahl zulässiger Vorauthentifizierungsversuche fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Dieses Netzwerk arbeitet mit Vorauthentifizierung“ ausgewählt wurde.
Proxy-Typ	Diese Einstellung legt den Typ der Proxy-Konfiguration für das Wi-Fi-Profil fest. Diese Einstellung gilt nur für Windows 10 Mobile-Geräte.
PAC-URL	Diese Einstellung gibt die URL für den Webserver an, der die PAC-Datei hostet, einschließlich PAC-Dateinamen im Format http://<web_server_URL>/<filename>.pac. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „PAC-Konfiguration“ gesetzt ist.
Adresse	Diese Einstellung gibt den Servernamen und Port für den Netzwerk-Proxy an. Verwenden Sie das Format „Host:Port“ (z. B. server01.beispiel.com:123). Der Host muss einer der folgenden sein: • Ein registrierter Name, z. B ein Servername, FQDN oder ein einzelner Etikettenname (z. B. "server01" anstatt server01.beispiel.com) • Eine IPv4- oder IPv6-Adresse Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Manuelle Konfiguration“ gesetzt ist.
Web-Proxy automatisch erkennen	Diese Einstellung gibt an, ob das WPAD-Protokoll (Web Proxy Autodiscovery Protocol) für die Proxy-Suche aktiviert werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Web-Proxy automatisch erkennen“ gesetzt ist.
Überprüfung der Internetverbindung deaktivieren	Diese Einstellung legt fest, ob Überprüfungen der Internetverbindung deaktiviert werden sollen.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen.

Einrichten von geschäftlichen VPNs für Geräte

Mithilfe von VPN-Profilen können Sie festlegen, wie iOS-, iPadOS-, macOS-, Samsung Knox- und Windows 10-Geräte eine Verbindung zu einem geschäftlichen VPN aufbauen. Sie können Benutzerkonten, Benutzergruppen oder Gerätegruppen ein VPN-Profil zuweisen.

Um eine Verbindung zu einem geschäftlichen VPN für andere Android-Geräte als Samsung Knox herzustellen, können Sie die VPN-Einstellungen mithilfe der App-Konfigurationseinstellungen für eine VPN-App konfigurieren, oder Benutzer können die VPN-Einstellungen auf ihren Geräten manuell konfigurieren.

Gerät	App- und Netzwerkverbindungen
iOS und iPadOS	Geschäftliche und private Apps können die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Sie können Per App VPN für ein VPN-Profil aktivieren, um das Profil nur auf die festgelegten geschäftlichen Apps anzuwenden. Sie können VPN bei Bedarf aktivieren, damit Geräte automatisch eine Verbindung zu einem VPN in einer bestimmten Domäne herstellen. Sie können z. B. die Domäne Ihres Unternehmens angeben, um Benutzern den Zugriff auf den Inhalt Ihres Intranets mithilfe von VPN bei Bedarf zu gestatten.
macOS	Konfigurieren Sie VPN-Profile, um das Herstellen einer Verbindung zu Ihrem Unternehmensnetzwerk über Apps zu ermöglichen. Sie können VPN bei Bedarf aktivieren, damit Geräte automatisch eine Verbindung zu einem VPN in einer bestimmten Domäne herstellen. Sie können z. B. die Domäne Ihres Unternehmens angeben, um Benutzern den Zugriff auf den Inhalt Ihres Intranets mithilfe von VPN bei Bedarf zu gestatten.
Samsung Knox	Auf Samsung Knox-Geräten, die über Android Enterprise- oder Samsung Knox Workspace-Aktivierungen verfügen, können geschäftliche Apps die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Sie können Per App VPN aktivieren, um das Profil nur auf die festgelegten geschäftlichen Apps anzuwenden. Sie müssen eine unterstützte VPN-Client-App mit KNOX SDK auf dem Gerät installieren.
Windows 10	Konfigurieren Sie VPN-Profile, um das Herstellen einer Verbindung zu Ihrem Unternehmensnetzwerk über Apps zu ermöglichen. Im VPN-Profil können Sie eine Liste von Apps angeben, die das VPN verwenden müssen.

Als Alternative zum Erstellen eines VPN-Profils können Sie CylanceGATEWAY verwenden, um ein Zero-Trust-Netzwerkzugriffsprofil (ZTNA) zu erstellen, das von Geräten als VPN-Anbieter erkannt wird. CylanceGATEWAY vertraut standardmäßig nichts und niemandem. Weitere Informationen finden Sie unter Integration von BlackBerry UEM in CylanceGATEWAY zum Erstellen eines ZTNA-Profils.

Erstellen eines VPN-Profils

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen vom VPN-Verbindungstyp und dem Authentifizierungstyp ab, die Sie ausgewählt haben. Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben.

Als Alternative zum Erstellen eines VPN-Profils können Sie CylanceGATEWAY verwenden, um ein Zero-Trust-Netzwerkzugriffsprofil (ZTNA) zu erstellen, das von Geräten als VPN-Anbieter erkannt wird. CylanceGATEWAY vertraut standardmäßig nichts und niemandem. Weitere Informationen finden Sie unter Integration von BlackBerry UEM in CylanceGATEWAY zum Erstellen eines ZTNA-Profils.

Bevor Sie beginnen:

- Wenn Geräte die zertifikatbasierte Authentifizierung für geschäftliche VPN-Verbindungen nutzen, erstellen Sie ein Profil mit Zertifizierungsstellenzertifikat, und weisen Sie es Benutzerkonten, Benutzergruppen oder Gerätegruppen zu. Um Client-Zertifikate an Geräte zu senden, erstellen Sie ein SCEP-Profil, ein Profil für

ein freigegebenes Zertifikat oder ein Profil für Benutzeranmeldeinformationen, das Sie mit dem VPN-Profil verknüpfen.

- Erstellen Sie ein Proxy-Profil für iOS-, iPadOS-, macOS- und Samsung Knox-Geräte, die einen Proxy-Server verwenden, das mit dem VPN-Profil verknüpft werden soll.
- Fügen Sie für Samsung Knox-Geräte die geeignete VPN-Client-App der App-Liste hinzu, und weisen Sie sie Benutzerkonten, Benutzergruppen oder Gerätegruppen zu. Als VPN-Client-Apps werden Cisco AnyConnect und Juniper unterstützt.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > VPN**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das VPN-Profil ein. Diese Informationen werden auf den Geräten angezeigt.
5. Klicken Sie auf die Registerkarte für einen Gerätetyp, um die zutreffenden Einstellungen zu konfigurieren. Weitere Informationen finden Sie in den VPN-Profileinstellungen für iOS und macOS, Android und Windows.

   Wenn Ihr Unternehmen verlangt, dass Benutzer einen Benutzernamen und ein Kennwort für den Zugriff auf das VPN-Netzwerk eingeben, geben Sie im Feld **Benutzername** `%UserName%` ein.
6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Wi-Fi-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

iOS und macOS: VPN-Profileinstellungen

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
Profil anwenden auf	Diese Einstellung gibt an, ob das VPN-Profil auf einem macOS-Gerät für das Benutzerkonto oder das Gerät gilt.
Verbindungstyp	Diese Einstellung legt den Verbindungstyp fest, den ein Gerät für ein VPN-Gateway verwendet. Bei einigen Verbindungstypen müssen die Benutzer außerdem die entsprechende VPN-App auf dem Gerät installieren. Wenn Sie „IKEv2 Immer An“ wählen, gelten für viele Einstellungen separate Werte für Mobilfunk- und Wi-Fi-Verbindungen.
VPN-Bundle-ID	Diese Einstellung legt die Bundle-ID der VPN-App für ein benutzerdefiniertes SSL-VPN fest. Die Bundle-ID wird im umgekehrten DNS-Format angegeben (beispielsweise „com.example.VPNapp“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.
Server	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
Benutzerdefinierte Schlüsselwertepaare	Diese Einstellung legt die Schlüssel und die verknüpften Werte für das benutzerdefinierte SSL-VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.
Anmeldegruppe oder Domäne	Diese Einstellung legt die Anmeldegruppe oder -domäne fest, die das VPN-Gateway verwendet, um ein Gerät zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SonicWALL Mobile Connect“ gesetzt ist.
Bereich	Diese Einstellung legt den Namen des Authentifizierungsbereichs fest, den das VPN-Gateway verwendet, um ein Gerät zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ oder „Pulse Secure“ gesetzt ist.
Rolle	Diese Einstellung legt den Namen der Benutzerrolle fest, den ein VPN-Gateway verwendet, um die Netzwerkressourcen zu überprüfen, auf die ein Gerät zugreifen kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ oder „Pulse Secure“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest. Die Einstellung „Verbindungstyp“ legt fest, welche Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird.
EAP-Plug-Ins	Diese Einstellung legt die Authentifizierungs-Plug-Ins für das VPN fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ oder „PPTP“ und die Einstellung „Authentifizierungstyp“ auf „RSA SecurID“ gesetzt ist.
Authentifizierungsprotokoll	Diese Einstellung legt die Authentifizierungsprotokolle für das VPN fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ oder „PPTP“ und die Einstellung „Authentifizierungstyp“ auf „RSA SecurID“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Kennwort“ gesetzt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
Gruppenname	Diese Einstellung legt den Gruppennamen für das VPN-Gateway fest. Diese Einstellung gilt nur unter den folgenden Bedingungen: • „Anschlusstyp“ ist eingestellt auf „Cisco AnyConnect“. • Die Einstellung „Anschlusstyp“ ist auf „IPsec“ und die Einstellung „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt.
Gemeinsamer geheimer Schlüssel	Diese Einstellung legt den gemeinsamen geheimen Schlüssel für die VPN-Authentifizierung fest. Diese Einstellung gilt nur unter den folgenden Bedingungen: • „Anschlusstyp“ ist eingestellt auf „L2TP“. • Die Einstellung „Anschlusstyp“ ist auf „IPsec“ und die Einstellung „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt. • Die Einstellung „Anschlusstyp“ ist auf „IKEv2“ oder „IKEv2 Immer An“ und die Einstellung „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel“ gesetzt.
Profil für freigegebenes Zertifikat	Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Clientzertifikat fest, das ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Clientzertifikat für die VPN-Authentifizierung abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung mit dem VPN abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
Verschlüsselungsstufe	Diese Einstellung legt die Stufe der Datenverschlüsselung für die VPN-Verbindung fest. Wenn diese Einstellung auf „Automatisch“ gesetzt ist, sind alle verfügbaren Verschlüsselungsstärken zulässig. Wenn diese Einstellung auf „Maximum“ gesetzt ist, ist nur die maximale Verschlüsselungsstärke zulässig. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „PPTP“ gesetzt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
Netzwerkverkehr durch VPN leiten	Diese Einstellung legt fest, ob der gesamte Netzwerkverkehr durch die VPN-Verbindung gesendet werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ oder „PPTP“ gesetzt ist.
Hybrid-Authentifizierung verwenden	Diese Einstellung legt fest, ob ein serverseitiges Zertifikat für die Authentifizierung verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und der „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/ Gruppenname“ gesetzt ist.
Zur Kennworteingabe auffordern	Diese Einstellung legt fest, ob ein Gerät den Benutzer zur Eingabe eines Kennworts auffordert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und der „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/ Gruppenname“ gesetzt ist.
Zur PIN-Eingabe auffordern	Diese Einstellung legt fest, ob das Gerät den Benutzer zur Eingabe einer PIN auffordert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ gesetzt ist, und die Einstellung für den „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“, „SCEP“ oder „Benutzeranmeldeinformationen“ gesetzt ist.
Remote-Adresse	Diese Einstellung legt die IP-Adresse bzw. den Hostnamen des VPN-Servers fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Lokale ID	Diese Einstellung legt die Identität des IKEv2-Clients in einem der folgenden Formate fest: FQDN, UserFQDN, Adresse und ASN1DN. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Remote-ID	Diese Einstellung legt die Remote-ID des IKEv2-Clients in einem der folgenden Formate fest: FQDN, Benutzer-FQDN, Adresse oder ASN1DN. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
VPN bei Bedarf aktivieren	Diese Einstellung legt fest, ob ein Gerät automatisch beim Zugriff auf bestimmte Domänen eine VPN-Verbindung herstellen kann. Diese Einstellung betrifft geschäftliche Apps auf iOS- und iPadOS-Geräten. Diese Einstellung gilt nur unter den folgenden Bedingungen: • Die Einstellung „Verbindungstyp“ ist auf „IPsec“, „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ und der „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“, „SCEP“ oder „Benutzeranmeldeinformationen“ gesetzt. • Die Einstellung „Anschlusstyp“ ist auf „IKEv2“ und der „Authentifizierungstyp“ auf „Gemeinsames Zertifikat“ gesetzt.
Domänen- oder Hostnamen, die "VPN auf Abruf" verwenden können	Diese Einstellung legt die Domänen und die verknüpften Aktionen für VPN bei Bedarf fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.
Regeln für „VPN bei Bedarf“ für iOS 7.0 und höher	Diese Einstellung legt die Verbindungsanforderungen für VPN bei Bedarf fest. Sie müssen einen oder mehrere Schlüssel aus dem Beispiel für das Nutzlastformat verwenden. Diese Einstellung überschreibt die Einstellung „Domänen- oder Hostnamen, die VPN bei Bedarf verwenden können“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.
Verbindung bei Leerlauf trennen	Diese Einstellung legt fest, ob die VPN-Verbindung getrennt wird, falls sie für einen bestimmten Zeitraum inaktiv ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.
Verbindung gemäß Leerlauf-Timer trennen	Diese Einstellung gibt die Leerlaufzeit in Sekunden an, nach der die VPN-Verbindung getrennt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindung bei Leerlauf trennen“ ausgewählt wurde.
Benutzer dürfen VPN nicht bei Bedarf deaktivieren	Diese Einstellung legt fest, ob der Benutzer das VPN bei Bedarf deaktivieren kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“, „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
Lokales Netzwerk ausschließen	Diese Einstellung legt fest, ob lokaler Netzwerkdatenverkehr von der Verwendung der VPN-Verbindung ausgenommen wird. Wenn die Einstellung „Alle Netzwerke einschließen“ ebenfalls ausgewählt ist, wird kein lokaler Netzwerkdatenverkehr über das VPN weitergeleitet.
Alle nicht standardmäßigen Weiterleitungen haben Vorrang vor allen lokal definierten Weiterleitungen	Diese Einstellung legt fest, ob die nicht standardmäßigen Weiterleitungen für das VPN Vorrang vor lokal definierten Weiterleitungen haben. Wenn die Einstellung „Alle Netzwerke einschließen“ ebenfalls ausgewählt ist, wird diese Einstellung ignoriert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist.
Alle Netzwerke einschließen	Diese Einstellung legt fest, ob der gesamte Netzwerkverkehr über das VPN weitergeleitet werden soll. Wenn auch „Lokales Netzwerk ausschließen“ ausgewählt ist, wird der lokale Netzwerkverkehr nicht über das VPN geleitet. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13 und höher.
Festgelegter Anbieter	Diese Einstellung gibt einen festgelegten VPN-Anbieter an. Wenn der VPN-Anbieter als Systemerweiterung implementiert ist, ist diese Einstellung erforderlich. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“, „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist.
Deaktivierung der automatischen Verbindung durch Benutzer zulassen	Diese Einstellung legt fest, ob Benutzer die VPN-Verbindung deaktivieren können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist.
Gleiche Tunnelkonfiguration für Mobilfunk und Wi-Fi verwenden	Diese Einstellung legt fest, ob Sie separate VPN-Einstellungen für das Gerät festlegen möchten, je nachdem, ob das Gerät Daten über ein Mobilfunknetz oder ein Wi-Fi-Netzwerk sendet. Wenn diese Einstellung nicht ausgewählt ist, können Sie unterschiedliche Mobilfunk- und Wi-Fi-Einstellungen im selben Profil festlegen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist.
xAuth aktivieren	Diese Einstellung legt fest, ob das VPN die erweiterte Authentifizierung (xAuth) unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
TLS-Mindestversion	Diese Einstellung gibt die minimale TLS-Version an, die Geräte für die EAP-TLS-Authentifizierung verwenden. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.
Höchste unterstützte TLS-Version	Diese Einstellung gibt die höchste unterstützte TLS-Version an, die Geräte für die EAP-TLS-Authentifizierung verwenden. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.
Zertifikattyp	Diese Einstellung gibt den Zertifikattyp an, der für die IKEv2-Computerauthentifizierung verwendet wird. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.
Allgemeiner Name des Serverzertifikatausstellers	Diese Einstellung gibt den allgemeinen Namen der Zertifizierungsstelle an, die das Zertifikat ausgestellt hat, das der IKE-Server an das Gerät sendet. Wenn Sie xAuth mithilfe eines Zertifikats aktivieren, ist diese Einstellung erforderlich. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.
Allgemeiner Name des Serverzertifikats	Diese Einstellung gibt den allgemeinen Namen des Serverzertifikats an, das der IKE-Server an das Gerät sendet. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.
Keep-alive-Intervall	Diese Einstellung legt fest, wie häufig ein Gerät ein Keep-alive-Paket sendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
MOBIKE deaktivieren	Diese Einstellung legt fest, ob MOBIKE deaktiviert ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
IKEv2-Umleitung deaktivieren	Diese Einstellung legt fest, ob die IKEv2-Umleitung deaktiviert ist. Wenn diese Einstellung nicht aktiviert ist, wird die IKEv2-Verbindung umgeleitet, wenn eine Umleitungsanfrage vom Server empfangen wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Perfekte Geheimhaltung bei der Weiterleitung aktivieren	Diese Einstellung legt fest, ob das VPN PFS unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
NAT-Keep-alive aktivieren	Diese Einstellung legt fest, ob das VPN NAT-Keep-alive-Pakete unterstützt. Keep-alive-Pakete werden zur Aufrechterhaltung der NAT-Zuordnungen für IKEv2-Verbindungen verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
NAT-Keep-alive-Intervall	Diese Einstellung legt fest, wie häufig ein Gerät ein NAT-Keep-alive-Paket sendet (in Sekunden). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt und die Einstellung „NAT-Keep-alive aktivieren“ ausgewählt ist.
Interne IPv4- und IPv6-IKEv2-Subnetze verwenden	Diese Einstellung legt fest, ob das VPN die Attribute INTERNAL_IP4_SUBNET und INTERNAL_IP6_SUBNET der IKEv2-Konfiguration verwenden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Allgemeiner Name des Serverzertifikats	Diese Einstellung gibt den allgemeinen Namen in dem Zertifikat an, das der IKE-Server an das Gerät sendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Allgemeiner Name des Serverzertifikatausstellers	Diese Einstellung gibt den allgemeinen Namen des Zertifikatsausstellers in dem Zertifikat an, das der IKE-Server an das Gerät sendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Zertifikatswiderrufprüfung aktivieren	Diese Einstellung gibt an, ob der Versuch einer Zertifikatswiderrufprüfung für das Serverzertifikat erfolgt. Die Prüfung schlägt nicht fehl, wenn keine Reaktion erfolgt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Fallback aktivieren	Diese Einstellung legt fest, ob das Gerät einen VPN-Tunnel über das Mobilfunknetz einrichten kann, wenn Wi-Fi Assist aktiviert ist. Diese Einstellung gilt nur für Geräte mit iOS und iPadOS 13 oder höher und erfordert, dass der Server mehrere Tunnel für einzelne Benutzer unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Untergeordnete Sicherheitszuordnungsparar anwenden	Diese Einstellung gibt an, ob untergeordnete Sicherheitszuordnungsparameter angewendet werden sollen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
IKE-Sicherheitszuordnungsparameter anwenden	Diese Einstellung gibt an, ob IKE-Sicherheitszuordnungsparameter angewendet werden sollen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
MTU	Diese Einstellung gibt die maximale Übertragungseinheit in Byte an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist.
Mailbox	Diese Einstellung legt fest, ob Verbindungen zum Mailbox-Dienst über den VPN-Tunnel gesendet, außerhalb des VPN-Tunnels gesendet oder blockiert werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Das gilt nur für Wi-Fi-Verbindungen.
AirPrint	Diese Einstellung legt fest, ob AirPrint-Verbindungen über den VPN-Tunnel gesendet, außerhalb des VPN-Tunnels gesendet oder blockiert werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Das gilt nur für Wi-Fi-Verbindungen.
Datenverkehr von Captive-Websheet außerhalb des VPN-Tunnels zulassen	Diese Einstellung legt fest, ob Datenverkehr von Captive Websheets außerhalb des VPN-Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Das gilt nur für Wi-Fi-Verbindungen.
Datenverkehr sämtlicher Captive-Netzwerk-Apps außerhalb des VPN-Tunnels zulassen	Diese Einstellung legt fest, ob Datenverkehr von allen Captive-Netzwerk-Apps außerhalb des VPN-Tunnels gesendet werden kann. Wenn diese Einstellung nicht aktiviert ist, können Sie einzelne Apps angeben, für die Datenverkehr außerhalb des Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Das gilt nur für Wi-Fi-Verbindungen.
Datenverkehr dieser Apps ist außerhalb des VPN-Tunnels zulässig	Diese Einstellung legt einzelne Captive-Netzwerk-Apps fest, für die Datenverkehr außerhalb des Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Das gilt nur für Wi-Fi-Verbindungen.
App-Datenverkehr außerhalb des VPN-Tunnels zulassen	Diese Einstellung legt Apps fest, deren Datenverkehr außerhalb des Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Das gilt nur für Wi-Fi-Verbindungen.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
DH-Gruppe	Diese Einstellung gibt die DH-Gruppe an, die ein Gerät zur Generierung des Schlüssels verwendet. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.
Verschlüsselungsalgorithmu	Diese Einstellung legt den IKE-Verschlüsselungsalgorithmus fest. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.
Integritätsalgorithmus	Diese Einstellung legt den IKE-Integritätsalgorithmus fest. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.
Schlüsseländerungsintervall	Diese Einstellung legt die Lebensdauer der IKE-Verbindung fest. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.
Per App VPN aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway Per App VPN unterstützt. Mit dieser Funktion kann die Belastung im VPN einer Organisation reduziert werden. So könnten Sie beispielsweise festlegen, dass nur ein bestimmter geschäftlicher Datenverkehr, wie etwa der Zugriff auf Anwendungsserver oder Webseiten, über das VPN abgewickelt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“, „Benutzerdefiniert“, „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Zulassen, dass Apps automatisch eine Verbindung herstellen	Diese Einstellung legt fest, ob mit Per App VPN verknüpfte Apps die VPN-Verbindung automatisch starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Safari-Domänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung in Safari starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Kalenderdomänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung im Kalender starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.

iOS, iPadOS und macOS: VPN-Profileinstellung	Beschreibung
Kontaktdomänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung in Kontakten starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
E-Mail-Domänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung im E-Mail-Programm starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Zugeordnete Domänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung auf dem Gerät starten können. Die Domänen müssen auch in der Datei „apple-app-site-association“ enthalten sein. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Ausgeschlossene Domänen	Diese Einstellung gibt Domänen an, die am Starten der VPN-Verbindung auf dem Gerät gehindert werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Datenverkehrs-Tunneling	Diese Einstellung legt fest, ob das VPN den Verkehr in der Anwendungsschicht oder IP-Schicht tunnelt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.

Android: VPN-Profileinstellungen

Die folgenden VPN-Profile werden nur auf Samsung Knox-Geräten unterstützt.

Android: VPN-Profileinstellung	Beschreibung
Serveradresse	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.
VPN-Typ	Diese Einstellung legt fest, ob ein Gerät IPsec oder SSL verwendet, um eine Verbindung mit dem Mailserver aufzubauen. Der Juniper-VPN-App unterstützt nur SSL.
Benutzerauthentifizierung erforderlich	Diese Einstellung legt fest, ob ein Gerät einen Benutzernamen und ein Kennwort zum Herstellen einer Verbindung mit dem VPN-Server bereitstellen muss.

Android: VPN-Profileinstellung	Beschreibung
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.
Kennwort	Diese Einstellung legt das Kennwort fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.
Split-Tunnel-Typ	Diese Einstellung legt fest, ob ein Gerät Split-Tunneling verwenden kann, um das VPN-Gateway zu umgehen, sofern dies vom VPN-Gateway unterstützt wird. Wenn der VPN-Typ auf „IPsec“ festgelegt ist, muss diese Einstellung auf „Deaktiviert“ festgelegt werden.
Weiterleitungsrouten	Diese Einstellung legt die Route(n) zum Umgehen des VPN-Gateways fest. Sie können eine oder mehrere IP-Adressen angeben. Diese Einstellung ist nur dann gültig, wenn „VPN-Typ“ auf „SSL“ und der „Split-Tunnel-Typ“ auf „Manuell“ gesetzt ist.
DPD	Diese Einstellung legt fest, ob DPD aktiviert ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Version	Diese Einstellung gibt die Version des IKE-Protokolls zur Verwendung mit der VPN-Verbindung an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für die IPsec-VPN-Verbindung fest. Die Einstellung „IKE-Version“ legt fest, welche IPsec-Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
ID-Typ der IPsec-Gruppe	Diese Einstellung legt den IPsec-Gruppen-ID-Typ für die VPN-Verbindung fest. Die Einstellung „IPsec-Authentifizierungstyp“ legt fest, welche IPsec-Gruppen-ID-Typen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Wird für „IPsec-Authentifizierungstyp“ die Einstellung „Zertifikat“ verwendet, dann wird diese Einstellung automatisch auf „Standard“ festgelegt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.

Android: VPN-Profileinstellung	Beschreibung
IPsec-Gruppen-ID	Diese Einstellung legt die IPsec-Gruppen-ID für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
Schlüsselaustauschmodus IKE-Phase-1	Diese Einstellung legt den Austauschmodus für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Lebensdauer	Diese Einstellung legt die Lebensdauer der IKE-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Verschlüsselungsalgorithmus	Diese Einstellung gibt den für eine IKE-Verbindung verwendeten Verschlüsselungsalgorithmus an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Integritätsalgorithmus	Diese Einstellung gibt den für eine IKE-Verbindung verwendeten Integritätsalgorithmus an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ und die „IKE-Version“ auf „IKEv2“ gesetzt ist.
IPsec DH-Gruppe	Diese Einstellung gibt die DH-Gruppe an, die ein Gerät zur Generierung des Schlüssels verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Parameter	Diese Einstellung legt die IPsec-Parameter für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
Perfekte Geheimhaltung bei der Weiterleitung	Diese Einstellung legt fest, ob das VPN-Gateway PFS unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
MOBIKE aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway MOBIKE unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.

Android: VPN-Profileinstellung	Beschreibung
IPsec-Lebensdauer	Diese Einstellung legt die Lebensdauer der IPsec-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Verschlüsselungsalgorithmu	Diese Einstellung legt den IPsec-Verschlüsselungsalgorithmus für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Integritätsalgorithmus	Diese Einstellung legt den IPsec-Integritätsalgorithmus für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ und die „IKE-Version“ auf „IKEv2“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.
SSL-Algorithmus	Diese Einstellung gibt den für eine SSL-VPN-Verbindung erforderlichen Verschlüsselungsalgorithmus an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.
UID-/PID-Informationen anhängen	Diese Einstellung gibt an, ob UID/PID-Informationen an Pakete angehängt werden, die an den VPN-Client gesendet werden. Diese Einstellung muss für die Cisco AnyConnect VPN-App aktiviert werden.
Verkettung unterstützen	Diese Einstellung legt fest, wie die VPN-Verkettung unterstützt wird.
Typ der Anbieterzeichenfolge	Diese Einstellung legt die Schlüsselwertpaare oder die JSON-Zeichenfolge für das VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters.
Schlüsselwertpaare des Anbieters	Diese Einstellung legt die Schlüssel und die verknüpften Werte für das VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Anbieterzeichenfolge“ auf „Schlüsselwertpaare des Anbieters“ gesetzt ist.
JSON-Wert des Anbieters	Diese Einstellung legt die Konfigurationsdaten für die VPN-App des Anbieters im .json-Format fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Anbieterzeichenfolge“ auf „JSON-Wert des Anbieters“ gesetzt ist.

Android: VPN-Profileinstellung	Beschreibung
Paket-ID des VPN-Clients	Diese Einstellung legt die Paket-ID der VPN-App fest.
Verbindung nach Fehler automatisch wiederherstellen	Diese Einstellung legt fest, ob die VPN-Verbindung nach Verbindungsverlust automatisch neu hergestellt werden soll.
FIPS-Modus aktivieren	Diese Einstellung legt fest, ob FIPS aktiviert ist. Durch Aktivieren des FIPS-Modus wird sichergestellt, dass nur FIPS-geprüfte Kryptografiealgorithmen für die VPN-Verbindung verwendet werden.
Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich	Diese Einstellung gibt an ob Samsung Knox-Geräte eine VPN-Verbindung für alle Apps im geschäftlichen Bereich oder nur für bestimmte Apps verwenden. • „Containerweites VPN“ verwendet eine VPN-Verbindung für alle Apps im geschäftlichen Bereich auf dem Gerät. • „Per App VPN“ verwendet nur für die angegebenen Apps eine VPN-Verbindung.
Apps, die VPN-Verbindung verwenden dürfen	Diese Einstellung gibt die Apps im geschäftlichen Bereich an, die eine VPN-Verbindung verwenden können. Sie können Apps aus einer Liste verfügbarer Apps auswählen oder die App-Paket-ID angeben. Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Per App VPN“ gesetzt ist.
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.

Windows 10: VPN-Profileinstellungen

Windows: VPN-Profileinstellung	Beschreibung
Verbindungstyp	Diese Einstellung legt den Verbindungstyp fest, den ein Windows 10-Gerät für ein VPN verwendet.
Server	Diese Einstellung gibt die öffentliche oder routbare IP-Adresse oder den DNS-Namen des VPN an. Diese Einstellung kann auf die externe IP eines VPN oder eine virtuelle IP einer Serverfarm hinweisen. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist.
Server-URL-Liste	Diese Einstellung gibt eine durch Kommas getrennte Liste von Servern mit URL, Hostname oder IP-Format an. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ nicht auf „Microsoft“ gesetzt ist.

Windows: VPN-Profileinstellung	Beschreibung
Typ der Routingrichtlinie	Diese Einstellung legt den Typ der Routingrichtlinie fest. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist.
Integrierter Protokolltyp	Diese Einstellung legt den Typ der Routingrichtlinie für das VPN fest. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist.
Authentifizierung	Diese Einstellung gibt die Authentifizierungsmethode für das systemeigene VPN an. Die Einstellung „Integrierter Protokolltyp“ legt fest, welche Authentifizierungsmethoden unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird.
EAP-Konfiguration	Diese Einstellung legt die XML der EAP-Konfiguration fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „EAP“ gesetzt ist.
Benutzermethode	Diese Einstellung gibt an, dass der Typ „Benutzermethode“ zur Authentifizierung verwendet werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „Benutzermethode“ gesetzt ist.
Gerätemethode	Diese Einstellung gibt an, dass der Typ „Gerätemethode“ zur Authentifizierung verwendet werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „Gerätemethode“ gesetzt ist.
Benutzerdefinierte Konfiguration	Diese Einstellung gibt das HTML-codierte XML-Blob für eine SSL-VPN-Plug-In-spezifische Konfiguration an, einschließlich Authentifizierungsdaten, die an das Gerät gesendet werden, um sie für SSL-VPN-Plug-Ins verfügbar zu machen. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ nicht auf „Microsoft“ gesetzt ist.
Name der Plug-In-Paketfamilie	Diese Einstellung legt den Namen der Paketfamilie des kundenspezifischen SSL-VPN fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Manuelle Verbindungsdefinition“ gesetzt ist.
Vorinstallierter Schlüssel L2TP	Diese Einstellung legt den vorinstallierten Schlüssel für L2TP-Verbindungen fest.
App-Auslöserliste	Diese Einstellung gibt eine Liste von Apps an, mit welchen die VPN-Verbindung gestartet wird.

Windows: VPN-Profileinstellung	Beschreibung
App-Auslöserliste > App-ID	Diese Einstellung gibt eine App für ein Per App VPN an. Mögliche Werte: • Name der Paketfamilie. Um den Namen der Paketfamilie zu erfahren, installieren Sie die App, und führen Sie den Windows PowerShell-Befehl `Get-AppxPackage` aus. • Installationsort der App. Zum Beispiel C:\WINDOWS\System\notepad.exe.
Routenliste	Diese Einstellung gibt eine Liste von Routen an, die das VPN verwenden kann. Wenn das VPN Split-Tunneling verwendet, ist eine Routenliste erforderlich.
Subnetzadresse	Diese Einstellung gibt die IP-Adresse des Zielpräfixes im IPv4- oder IPv6-Adressformat an.
Subnetzpräfix	Diese Einstellung gibt das Subnetzpräfix des Zielpräfixes an.
Ausschluss	Diese Einstellung gibt an, ob die hinzugefügte Weiterleitung auf eine VPN-Schnittstelle als Gateway oder eine physische Schnittstelle verweisen muss. Wenn Sie das Kontrollkästchen aktivieren, wird der Datenverkehr über die physische Schnittstelle geleitet. Wenn Sie das Kontrollkästchen nicht aktivieren, wird der Datenverkehr über das VPN geleitet.
Domänennamenliste	Diese Einstellung legt die NRPT-Regeln (Name Resolution Policy Table) für das VPN fest.
Domänenname	Diese Einstellung gibt den FQDN oder das Suffix der Domäne an.
DNS-Server	Diese Einstellung gibt die Liste der IP-Adressen der DNS-Server durch Kommas getrennt an.
Web-Proxyserver	Diese Einstellung gibt die IP-Adresse des Web-Proxyservers an.
VPN-Verwendung auslösen	Die Einstellung legt fest, ob diese Domänennamenregel die VPN-Verwendung auslöst.
Permanent	Diese Einstellung legt fest, ob die Domänennamenregel angewendet wird, wenn keine VPN-Verbindung besteht.
Filterliste für Verkehr	Diese Einstellung legt die Regeln fest, die Datenverkehr über das VPN zulassen.
Filterliste für Verkehr > App-ID	Diese Einstellung gibt eine App für einen App-basierten Verkehrsfilter an. Mögliche Werte: • Name der Paketfamilie. Um den Namen der Paketfamilie zu erfahren, installieren Sie die App, und führen Sie den Windows PowerShell-Befehl `Get-AppxPackage` aus. • Installationsort der App. Beispiel: `C:\Windows\System\Notepad.exe`. • Geben Sie „SSYSTEM“ ein, um zu ermöglichen, dass der Kernel-Treiber Datenverkehr über das VPN sendet (z. B. PING oder SMB).

Windows: VPN-Profileinstellung	Beschreibung
Protokoll	Diese Einstellung legt das vom VPN verwendete Protokoll fest.
Lokale Portbereiche	Diese Einstellung gibt die Liste der zulässigen lokalen Portbereiche getrennt durch Kommas an. Zum Beispiel 100-120, 200, 300-320.
Remote-Portbereiche	Diese Einstellung gibt die Liste der zulässigen Remote-Portbereiche getrennt durch Kommas an. Zum Beispiel 100-120, 200, 300-320.
Lokale Adressenbereiche	Diese Einstellung gibt die Liste der zulässigen lokalen IP-Adressenbereiche getrennt durch Kommas an.
Remote-Adressbereiche	Diese Einstellung gibt die Liste der zulässigen Remote-IP-Adressbereiche getrennt durch Kommas an.
Typ der Routingrichtlinie	Diese Einstellung gibt die Routingrichtlinie an, die vom Verkehrsfilter verwendet wird. Wenn die Einstellung „Tunnel erzwingen“ lautet, wird sämtlicher Datenverkehr über das VPN geleitet. Wenn die Einstellung „Split-Tunneling“ lautet, kann der Datenverkehr über das VPN oder das Internet geleitet werden.
Zugangsdaten speichern	Diese Einstellung gibt an, ob die Anmeldeinformationen, wann immer möglich, zwischengespeichert werden.
Immer ein	Diese Einstellung legt fest, ob die Geräte bei der Anmeldung automatisch eine Verbindung zum VPN herstellen, die erhalten bleibt, bis der Benutzer sie manuell trennt.
Sperrung	Mit dieser Einstellung wird angegeben, ob diese VPN-Verbindung verwendet werden muss, wenn das Gerät eine Verbindung mit einem Netzwerk herstellt. Wenn diese Einstellung aktiviert ist, gilt Folgendes: • Das Gerät bleibt mit dem VPN verbunden. Die Verbindung kann nicht getrennt werden. • Das Gerät muss mit diesem VPN verbunden sein, damit eine Netzwerkverbindung besteht. • Das Gerät kann nicht mit anderen VPN-Profilen verbunden werden oder diese ändern.
DNS-Suffix	Diese Einstellung gibt ein oder mehrere DNS-Suffixe durch Kommas getrennt an. Das erste DNS-Suffix in der Liste wird auch als primäre Verbindung für das VPN verwendet. Die Liste wird zur SuffixSearchList hinzugefügt.
Erkennung eines vertrauenswürdigen Netzwerks	Diese Einstellung gibt eine durch Kommas getrennte Zeichenfolge zur Identifizierung des vertrauenswürdigen Netzwerks an. Das VPN stellt keine automatische Verbindung her, wenn sich die Benutzer im Drahtlosnetzwerk ihrer Organisation befinden.
IP-Sicherheitseigenschaften	
Authentifizierungstransformationskonstanten	Diese Einstellung legt die Authentifizierungsebene eines VPN fest. Diese Einstellung muss mit der Einstellung auf dem VPN-Server übereinstimmen.

Windows: VPN-Profileinstellung	Beschreibung
Chiffriertransformationskon	Diese Einstellung legt die Verschlüsselungsstufe eines VPN fest. Diese Einstellung muss mit der Einstellung auf dem VPN-Server übereinstimmen.
Verschlüsselungsmethode	Diese Einstellung legt die Verschlüsselung der ersten Phase eines VPN fest. Diese Einstellung muss mit der Einstellung auf dem VPN-Server übereinstimmen.
Integritätsprüfungsmethode	Diese Einstellung legt die Authentifizierungsebene der ersten Phase eines VPN fest. Diese Einstellung muss mit der Einstellung auf dem VPN-Server übereinstimmen.
Diffie-Hellman-Gruppe	Diese Einstellung legt die Schlüsselgruppe eines VPN fest. Diese Einstellung muss mit der Einstellung auf dem VPN-Server übereinstimmen.
PFS-Gruppe	Diese Einstellung legt das Verschlüsselungsprotokoll Perfect Forward Secrecy fest, das für das VPN verwendet wird. Diese Einstellung muss mit der Einstellung auf dem VPN-Server übereinstimmen.
Proxy-Typ	Diese Einstellung legt den Typ der Proxy-Konfiguration für das VPN fest.
PAC-URL	Diese Einstellung gibt die URL für den Webserver an, der die PAC-Datei hostet, einschließlich PAC-Dateinamen. Zum Beispiel http://www.example.com/PACfile.pac. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „PAC-Konfiguration“ gesetzt ist.
Adresse	Diese Einstellung legt den FQDN oder die IP-Adresse eines Proxy-Servers fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Manuelle Konfiguration“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Client-Zertifikat für die VPN-Authentifizierung abzurufen.

Integration von BlackBerry UEM in CylanceGATEWAY zum Erstellen eines ZTNA-Profils

Alternativ zu einem VPN-Profil können Sie UEM in CylanceGATEWAY integrieren. CylanceGATEWAY ist eine Cloud-native Lösung, die Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA) gestützt auf künstliche Intelligenz (KI) bietet und für Ihren Cylance Endpoint Security-Mandanten aktiviert werden kann. Sie können CylanceGATEWAY in der Cylance-Verwaltungskonsole einrichten. Informationen zur Einrichtung von CylanceGATEWAY finden Sie unter Einrichten von BlackBerry Gateway in der Dokumentation zur Cylance Endpoint Security-Einrichtung. Wenn CylanceGATEWAY auf einem Gerät aktiviert ist, erstellen Sie ein ZTNA-Profil, das das Gerät als VPN-Anbieter erkennt. CylanceGATEWAY vertraut standardmäßig nichts und niemandem.

CylanceGATEWAY schützt die iOS-, Android-, Windows 10- bzw. 11- sowie macOS-Geräte Ihrer Benutzer, indem Sie Verbindungen zu Internetzielen blockieren können, mit denen die Geräte nicht kommunizieren sollen, selbst wenn das Gerät nicht mit Ihrem Netzwerk verbunden ist.

Zusätzlich zum Schutz von Geräten schützt CylanceGATEWAY den Zugriff auf das private Netzwerk und die Cloud-basierten Anwendungen Ihres Unternehmens, indem kontinuierlich analysiert wird, ob es sich um erwartetes Nutzungsverhalten der Benutzer oder um ungewöhnliches Verhalten handelt. Wenn der Prozentsatz

der anormalen Ereignisse einen festgelegten Schwellenwert überschreitet, kann CylanceGATEWAY die Netzwerkzugriffssteuerungsrichtlinie des Benutzers dynamisch außer Kraft setzen, um den Netzwerkzugriff zu blockieren und den Benutzer zur Authentifizierung aufzufordern, bevor er fortfahren kann.

CylanceGATEWAY Administratoren können konfigurieren, auf welche Internet- und privaten Netzwerkziele Benutzer zugreifen können und auf welche der Zugriff gesperrt ist.

Aktivieren und Zuweisen von Per-App-VPN-Einstellungen

Sie können VPN pro App auf iOS-, iPadOS-, Samsung Knox- und Windows-Geräten einrichten, um zu bestimmen, welche Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Per App VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (bspw. Zugriff auf Anwendungsserver oder Webseiten hinter der Firewall). In lokalen Umgebungen unterstützt diese Funktion auch die Privatsphäre des Benutzers und erhöht die Verbindungsgeschwindigkeit für persönliche Apps, indem der persönliche Datenverkehr nicht über das VPN gesendet wird.

Geräte	App-Einstellungen
iOS und iPadOS	Apps sind mit einem VPN-Profil verknüpft, wenn Sie die App oder App-Gruppe einem Benutzer, einer Benutzergruppe oder einer Gerätegruppe zuweisen.
Samsung Knox-Geräte mit Android Enterprise- und Samsung Knox Workspace-Aktivierungen	Apps werden im VPN-Profil der Einstellung „Apps, die VPN-Verbindung verwenden dürfen“ hinzugefügt.
Windows 10	Apps werden im VPN-Profil der Einstellung „App-Auslöserliste“ hinzugefügt.

Einer App oder einer App-Gruppe kann nur ein VPN-Profil zugewiesen werden.

BlackBerry UEM verwendet die folgenden Regeln, um zu bestimmen, welche VPN pro App-Einstellungen einer App auf iOS- und iPadOS-Geräten zugewiesen werden:

Per-App-VPN-Einstellungen	Vorrang
Falls direkt mit einer App verknüpft	Hat Vorrang vor Per-App-VPN-Einstellungen, die indirekt von einer App-Gruppe verknüpft sind.
Falls direkt mit einem Benutzer verknüpft	Haben Vorrang vor Per-App-VPN-Einstellungen, die indirekt von einer Benutzergruppe verknüpft sind.
Falls direkt einer erforderlichen App zugewiesen	Hat Vorrang vor Per-App-VPN-Einstellungen, die einer optionalen Instanz derselben App zugewiesen sind.

Per-App-VPN-Einstellungen	Vorrang
Falls mit dem Benutzergruppennamen verknüpft, der in der alphabetischen Liste vorher aufgeführt ist	Hat Vorrang, falls die folgenden Bedingungen erfüllt werden: • Eine App ist mehreren Benutzergruppen zugewiesen • Die gleiche App wird in den Benutzergruppen angezeigt • Die App wird auf die gleiche Art zugewiesen, entweder als einzelne App oder als App-Gruppe • Die App hat in allen Zuweisungen die gleiche Verfügbarkeit, entweder erforderlich oder optional Beispielsweise ist Cisco WebEx Meetings den Benutzergruppen Entwicklung und Marketing als optionale App zugewiesen. Ist ein Benutzer in beiden Gruppen vorhanden, werden die Per App VPN-Einstellungen für die Entwicklungsgruppe auf die WebEx Meetings-App für diesen Benutzer angewendet.

Wenn das Per App VPN-Profil einer Gerätegruppe zugewiesen ist, hat es für alle Geräte, die dieser Gerätegruppe angehören, Vorrang vor dem Per App VPN-Profil, das dem Benutzerkonto zugewiesen ist.

Einrichten von Proxy-Profilen für Geräte

Sie können festlegen, wie die Geräte einen Proxy-Server nutzen, um auf Webdienste im Internet oder auf ein geschäftliches Netzwerk zuzugreifen. Erstellen Sie für iOS-, iPadOS-, macOS- und Android-Geräte ein Proxy-Profil. Fügen Sie für Windows 10-Geräte die Proxy-Einstellungen im Wi-Fi- oder VPN-Profil hinzu.

Wenn nicht anders dargestellt, unterstützen Proxy-Profile Proxy-Server, die nur eine allgemeine Authentifizierung oder gar keine Authentifizierung verwenden.

Gerät	Proxy-Konfiguration
iOS und iPadOS	Erstellen Sie ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi- oder VPN-Profil. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Proxy-Profil zuweisen. Ein Proxy-Profil, das Benutzerkonten, Benutzergruppen oder Gerätegruppen zugewiesen wird, ist nur ein globaler Proxy für überwachte Geräte und hat Vorrang vor einem Proxy-Profil, das mit einem VPN- oder Wi-Fi-Profil verknüpft ist. Überwachte Geräte verwenden die globalen Proxy-Einstellungen für alle HTTP-Verbindungen.
macOS	Erstellen Sie ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi- oder VPN-Profil. Bei macOS gelten Profile für Benutzerkonten oder Geräte. Proxy-Profile gelten für Geräte.

Gerät	Proxy-Konfiguration
Android	Erstellen Sie für Android Enterprise-Geräte ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi-Profil. Auf Geräten mit Android, die über MDM-Steuerelemente- oder Privatsphäre des Benutzers-Aktivierungen verfügen, werden Wi-Fi-Profile mit Proxyeinstellungen nicht unterstützt.
Samsung Knox	Erstellen Sie ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi-, Enterprise-Konnektivitäts- oder VPN-Profil. Es gelten folgende Bedingungen: • Für die Wi-Fi-Profile werden nur Proxy-Profile mit manueller Konfiguration auf Knox-Geräten unterstützt. Proxy-Profile, die Sie mit Wi-Fi-Profilen verknüpfen, unterstützen Proxy-Server, die eine allgemeine Authentifizierung, NTLM oder gar keine Authentifizierung verwenden. • Für VPN- und Enterprise-Konnektivitätsprofile werden Proxy-Profile mit manueller Konfiguration auf Samsung Knox-Geräten mit Android Enterprise-Aktivierungen und Samsung Knox Workspace-Geräten mit Knox 2.5 und höher unterstützt. Proxy-Profile mit PAC-Konfiguration werden auf Samsung Knox-Geräten mit Android Enterprise-Aktivierungen und Knox Workspace-Geräten mit Knox-Version höher als 2.5 unterstützt. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Proxy-Profil zuweisen. Es gelten folgende Bedingungen: • Auf Knox Workspace-Geräten und Samsung Knox-Geräten mit Android Enterprise-Aktivierungen bestimmt das Profil die Browser-Proxy-Einstellungen des geschäftlichen Bereichs. • Auf Samsung Knox-MDM-Geräten bestimmt die Profilkonfiguration die Browser-Proxy-Einstellungen des Geräts. • PAC-Konfiguration wird auf Knox Workspace-Geräten mit Knox 2.5 und früher und Knox-MDM-Geräten nicht unterstützt.
Windows 10	Erstellen Sie ein Wi-Fi- oder VPN-Profil, und geben Sie die Proxy-Serverinformationen in den Profileinstellungen an. Es gelten folgende Bedingungen: • Wi-Fi-Proxy unterstützt nur manuelle Konfiguration und ist nur mit Windows 10 Mobile-Geräten kompatibel. • VPN-Proxy unterstützt PAC oder manuelle Konfiguration.

Erstellen eines Proxy-Profils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > Proxy**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Proxy-Profil ein.
5. Klicken Sie auf die Registerkarte eines Gerätetyps.
6. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Festlegen der Einstellungen für die PAC-Konfiguration	**a.** Klicken Sie in der Dropdown-Liste **Typ** auf **PAC-Konfiguration**. **b.** Geben Sie im Feld **PAC-URL** die URL für den Webserver an, der die PAC-Datei hostet, sowie den PAC-Dateinamen (zum Beispiel http://www.example.com/PACfile.pac). Die PAC-Datei sollte nicht auf einem Server gehostet werden, der UEM oder eine seiner Komponenten hostet.
Festlegen der Einstellungen zur manuellen Konfiguration	**a.** Klicken Sie in der Dropdown-Liste **Typ** auf **Manuelle Konfiguration**. **b.** Geben Sie im Feld **Host** den FQDN oder die IP-Adresse des Proxy-Servers ein. **c.** Geben Sie im Feld **Port** die Portnummer des Proxy-Servers ein. **d.** Wenn Ihr Unternehmen erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für die Verbindung zum Proxy-Server eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername** `%UserName%` ein. Wenn der Proxy-Server den Domänennamen zur Authentifizierung benötigt, verwenden Sie das Format *<domain>**<username>*.

7. Wiederholen Sie die Schritte 4 bis 6 für jeden Gerätetyp.
8. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Verknüpfen Sie das Proxy-Profil mit einem Wi-Fi-, VPN- oder Enterprise-Konnektivitätsprofil.
- Wenn Sie mehr als ein Proxy-Profil erstellen möchten, dann legen Sie nach Bedarf eine Rangfolge für die Profile fest. Die von Ihnen festgelegte Reihenfolge gilt nur, wenn Sie den Benutzergruppen oder Gerätegruppen ein Proxy-Profil zuweisen. Wählen Sie ein Profil aus, und klicken Sie auf ⇅, um das Profil in der Rangfolge nach oben oder unten zu verschieben. Klicken Sie auf **Speichern**.

Verwenden von BlackBerry Secure Connect Plus für Verbindungen mit geschäftlichen Ressourcen

Die BlackBerry Secure Connect Plus ist eine BlackBerry UEM-Komponente, die einen sicheren IP-Tunnel zwischen Apps und dem Netzwerk des Unternehmens bereitstellt.

- Auf Android Enterprise-Geräten verwenden alle geschäftlichen Apps den sicheren Tunnel.
- Für Samsung Knox Workspace-Geräte und Samsung Knox-Geräte mit Android Enterprise-Aktivierungen können Sie zulassen, dass alle Apps des geschäftlichen Bereichs den Tunnel nutzen oder festlegen, welche Apps „Per App VPN“ verwenden.
- Bei iOS- und iPadOS-Geräten können Sie zulassen, dass alle Apps den Tunnel nutzen oder festlegen, welche Apps „VPN pro App“ verwenden.

Hinweis: Wenn BlackBerry Secure Connect Plus in Ihrer Region nicht verfügbar ist, müssen Sie es manuell für Android-Geräte im Enterprise-Konnektivitätsprofil deaktivieren.

Über diesen sicheren IP-Tunnel haben Benutzer Zugriff auf Ressourcen hinter der Firewall Ihres Unternehmens, wobei die Sicherheit der Daten mithilfe von Standardprotokollen und durchgehender Verschlüsselung sichergestellt wird.

BlackBerry Secure Connect Plus und unterstützte Geräte erstellen einen sicheren IP-Tunnel, wenn dies die beste Wahl für eine Verbindung mit dem Netzwerk des Unternehmens ist. Ist einem Gerät ein Wi-Fi oder VPN-Profil

zugewiesen, und das Gerät hat Zugriff auf das geschäftliche Wi-Fi- bzw. VPN-Netzwerk, wird diese Methode zum Herstellen einer Verbindung verwendet. Stehen diese Möglichkeiten nicht zur Verfügung (z. B. wenn der Benutzer sich außerhalb des geschäftlichen Wi-Fi-Funkbereichs befindet), stellen BlackBerry Secure Connect Plus und das Gerät einen sicheren IP-Tunnel her.

Wenn Sie „Per-App-VPN“ für BlackBerry Secure Connect Plus für iOS- und iPadOS-Geräte konfigurieren, verwenden die konfigurierten Apps immer eine sichere Tunnelverbindung über BlackBerry Secure Connect Plus, auch wenn die App eine Verbindung zum geschäftlichen Wi-Fi-Netzwerk oder VPN herstellen kann, das in einem VPN-Profil festgelegt ist.

Unterstützte Geräte kommunizieren zur Herstellung des sicheren Tunnels über die BlackBerry Infrastructure mit BlackBerry UEM. Für jedes Gerät wird ein Tunnel erstellt. Der Tunnel unterstützt Standard-IPv4-Protokolle (TCP und UDP), und der IP-Datenverkehr, der zwischen Geräten und UEM gesendet wird, ist komplett mithilfe von AES256 verschlüsselt. Solange der Tunnel geöffnet ist, haben die Apps Zugriff auf Netzwerkressourcen. Sobald der Tunnel nicht mehr benötigt wird (zum Beispiel, wenn der Benutzer in den Empfangsbereich des geschäftlichen Wi-Fi-Netzwerks zurückkehrt), wird er geschlossen.

Beim Aktivieren von BlackBerry Secure Connect Plus führen Sie die folgenden Aktionen aus:

Schritt	Aktion
1	Vergewissern Sie sich, dass die BlackBerry UEM-Domäne im Unternehmen die Anforderungen zur Verwendung von BlackBerry Secure Connect Plus erfüllt.
2	Aktivieren Sie BlackBerry Secure Connect Plus im Standard-Enterprise-Konnektivitätsprofil oder in einem von Ihnen erstellten benutzerdefinierten Enterprise-Konnektivitätsprofil.
3	Optional: Legen Sie die DNS-Einstellungen für die BlackBerry Connectivity-App fest.
4	Wenn in Ihrer lokalen Umgebung Android Enterprise-Geräte und Samsung Knox Workspace-Geräte mit Aktivierung für BlackBerry Dynamics vorhanden sind, optimieren Sie die sicheren Tunnelverbindungen.
5	Weisen Sie das Enterprise-Konnektivitätsprofil Benutzerkonten und -gruppen zu.

Server- und Geräteanforderungen für BlackBerry Secure Connect Plus

Zur Verwendung von BlackBerry Secure Connect Plus muss die Umgebung des Unternehmens folgende Anforderungen erfüllen.

BlackBerry UEM-Domäne:

Umgebung	Anforderungen
Alle UEM-Umgebungen	• Die Firewall muss ausgehende Verbindungen über Port 3101 mit *<region>*.turnb.bbsecure.com und *<region>*.bbsecure.com zulassen. Wenn Sie UEM zur Verwendung eines Proxyservers konfigurieren, muss dieser Verbindungen über Port 3101 mit diesen Unterdomänen zulassen. • In jeder UEM-Instanz muss die BlackBerry Secure Connect Plus-Komponente ausgeführt werden. • Standardmäßig ist es Android Enterprise-Geräten nicht gestattet, BlackBerry Secure Connect Plus zum Herstellen einer Verbindung mit Google Play und zugrunde liegenden Services (com.android.providers.media, com.android.vending und com.google.android.apps.gcs) zu nutzen. Google Play bietet keine Proxyunterstützung. Android Enterprise-Geräte nutzen eine direkte Verbindung über das Internet zu Google Play. Diese Einschränkungen sind im Standardprofil für die Enterprise-Konnektivität sowie in allen von Ihnen neu erstellten Enterprise-Konnektivitätsprofilen konfiguriert. Es wird empfohlen, diese Einschränkungen beizubehalten. Wenn Sie die Einschränkungen entfernen, müssen Sie sich an den Google Play-Support wenden, um zu erfahren, welche Firewall-Konfiguration erforderlich ist, um Verbindungen zu Google Play über BlackBerry Secure Connect Plus zuzulassen. • Wenn Sie ein E-Mail-Profil zum Aktivieren von BlackBerry Secure Gateway für iOS-Geräte verwenden, empfiehlt es sich, Per App VPN für BlackBerry Secure Connect Plus zu konfigurieren.
Lokales UEM	• Wenn in Ihrer Umgebung Knox Workspace- und Android Enterprise-Geräte mit BlackBerry Dynamics-Apps vorhanden sind, siehe Optimieren von sicheren Tunnelverbindungen für Android-Geräte, die BlackBerry Dynamics-Apps verwenden. • Optional können Sie weitere BlackBerry Secure Connect Plus-Instanzen installieren, indem Sie mehr als eine BlackBerry Connectivity Node installieren. • Optional können Sie eine Servergruppe erstellen, um BlackBerry Secure Connect Plus-Datenverkehr an einen bestimmten regionalen Pfad zur BlackBerry Infrastructure zu leiten.
UEM Cloud	• Sie müssen BlackBerry Connectivity Node installieren oder auf die neueste Version aktualisieren. Wenn Sie BlackBerry Connectivity Node installieren oder aktualisieren, wird auch BlackBerry Secure Connect Plus installiert oder aktualisiert. Sie müssen sicherstellen, dass Sie BlackBerry Connectivity Node aktivieren, bevor Sie BlackBerry Secure Connect Plus aktivieren. • Wenn Sie die Daten, die zwischen BlackBerry Secure Connect Plus und der BlackBerry Infrastructure übertragen werden, über einen TCP-Proxyserver (transparent oder SOCKS v5) weiterleiten, können Sie die Proxy-Einstellungen über die BlackBerry Connectivity Node-Verwaltungskonsole konfigurieren (Allgemeine Einstellungen > Proxy).

Unterstützte Geräte:

Profil	Beschreibung
iOS und iPadOS	• Die Geräte müssen mit dem BlackBerry UEM Client aktiviert werden. Bei Apple-DEP-Geräten müssen Sie den UEM Client über UEM an Benutzer verteilen und dann die Benutzer anweisen, den UEM Client zu öffnen und den Einrichtungsvorgang abzuschließen. • Aktivierung mit MDM-Steuerelementen
Android Enterprise	Eine der folgenden Aktivierungsarten: • Nur geschäftlicher Bereich (Premium) • Geschäftlich und persönlich – vollständige Kontrolle (Premium) • Geschäftlich und persönlich – Benutzer-Datenschutz (Premium)

Samsung Knox Workspace	• Eine unterstützte Version von Samsung Knox.
	• Eine der folgenden Aktivierungsarten:
	  • Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)
	  • Geschäftlich und persönlich – Privatsphäre des Benutzers (Samsung Knox)

Enable BlackBerry Secure Connect Plus

Wenn Sie zulassen möchten, dass Geräte BlackBerry Secure Connect Plus verwenden, müssen Sie BlackBerry Secure Connect Plus in einem Enterprise-Konnektivitätsprofil aktivieren und das Profil Benutzern und Gruppen zuweisen.

Wenn dem Gerät nach der Aktivierung das Enterprise-Konnektivitätsprofil zugewiesen wird, installiert BlackBerry UEM die BlackBerry Connectivity-App auf dem Gerät (bei Android Enterprise-Geräten wird die App automatisch aus Google Play installiert; bei iOS- und iPadOS-Geräten wird die App automatisch aus dem App Store installiert).

Bevor Sie beginnen: Stellen Sie sicher, dass die UEM-Domäne Ihres Unternehmens die Anforderungen zur Verwendung von BlackBerry Secure Connect Plus erfüllt.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Netzwerke und Verbindungen > Enterprise-Konnektivität**.
2. Bearbeiten Sie ein vorhandenes Enterprise-Konnektivitätsprofil, oder erstellen Sie ein neues.
3. Wenn Sie eine oder mehrere Servergruppen erstellt haben, um BlackBerry Secure Connect Plus-Datenverkehr an einen spezifischen regionalen Pfad zur BlackBerry Infrastructure zu leiten, klicken Sie in der Dropdown-Liste **Servergruppe für BlackBerry Secure Connect Plus** auf die entsprechende Servergruppe.
4. Konfigurieren Sie die entsprechenden Werte für die Profileinstellungen jedes Gerätetyps. Weitere Informationen zu den einzelnen Profileinstellungen finden Sie unter Einstellungen für Enterprise-Konnektivitätsprofile.
5. Klicken Sie auf **Hinzufügen**.
6. Weisen Sie das Profil Benutzergruppen bzw. Benutzerkonten zu.

Wenn Sie fertig sind:

- Auf Android Enterprise- und Samsung Knox Workspace-Geräten werden Benutzer von der BlackBerry Connectivity-App aufgefordert, die Ausführung als VPN und den Zugriff auf private Schlüssel auf dem Gerät zuzulassen. Weisen Sie die Benutzer an, dieser Aufforderung nachzukommen. Gerätebenutzer können die App zum Anzeigen des Verbindungsstatus öffnen. Es sind keine weiteren Maßnahmen von den Benutzern erforderlich.

- Wenn Sie mehrere Enterprise-Konnektivitätsprofile erstellt haben, weisen Sie ihnen eine Rangordnung zu. Wählen Sie ein Profil aus, und klicken Sie auf ⇅, um das Profil in der Rangfolge nach oben oder unten zu verschieben. Klicken Sie auf **Speichern**.
- Wenn Sie ein Verbindungsproblem mit einem iOS-, iPadOS-, Android Enterprise- oder Knox Workspace-Gerät beheben müssen, kann der Benutzer Geräteprotokolle an die E-Mail-Adresse eines Administrators senden (der Benutzer gibt eine von Ihnen bereitgestellte E-Mail-Adresse an). Beachten Sie, dass die Anzeige der Protokolle mit Winzip nicht möglich ist. Es ist daher empfehlenswert, ein anderes Tool wie z. B. 7-Zip zu verwenden.
- Legen Sie optional die DNS-Einstellungen für die BlackBerry Connectivity-App fest.

Aktualisieren der BlackBerry Connectivity-App

Die neueste BlackBerry Connectivity-App ist in Google Play und von BlackBerry myAccount Software Downloads verfügbar.

- **Android-Benutzer:** Weisen Sie Gerätebenutzer an, auf die neuesten Versionen des BlackBerry UEM Client und der BlackBerry Connectivity-App zu aktualisieren, die unter Google Play verfügbar sind. Befolgen Sie für Geräte, die keinen Zugriff auf Google Play haben, die Anweisungen unter Aktualisieren der BlackBerry Connectivity-App für Samsung Knox Workspace- und Android Enterprise-Geräte, die keinen Zugriff auf Google Play haben.
- **Samsung Knox Workspace-Benutzer:**
  - Weisen Sie die Gerätebenutzer bei Knox-Geräten mit aktivierter Google Play-App-Verwaltung an, auf die neuesten Versionen des BlackBerry UEM Client und der BlackBerry Connectivity-App zu aktualisieren, die unter Google Play verfügbar sind. Stellen Sie in der UEM-Verwaltungskonsole sicher, dass die BlackBerry Connectivity-App auf „Alle Android-Geräte“ eingestellt ist, und weisen Sie sie den entsprechenden Benutzern und Gruppen zu.
  - Befolgen Sie bei Knox-Geräten, für die die Google Play-App-Verwaltung nicht aktiviert ist, die Anweisungen unter Aktualisieren der BlackBerry Connectivity-App für Samsung Knox Workspace- und Android Enterprise-Geräte, die keinen Zugriff auf Google Play haben.

Hinweis: Wenn Sie Zertifizierungsstellenzertifikat-Profile zur Verteilung von Zertifizierungsstellenzertifikaten auf Android- oder Knox Workspace-Geräte verwenden, stellen Sie sicher, dass die hochgeladenen Zertifikate entweder die Dateierweiterung .der haben oder PEM-codiert sind und die Dateierweiterung .pem haben. Zertifizierungsstellenzertifikate, die diese Anforderungen nicht erfüllen, können Verbindungsprobleme für die BlackBerry Connectivity-App verursachen.

Aktualisieren der BlackBerry Connectivity-App für Samsung Knox Workspace- und Android Enterprise-Geräte, die keinen Zugriff auf Google Play haben

Befolgen Sie die nachstehenden Anweisungen, um die BlackBerry Connectivity-App auf den Geräten der Benutzer auf die aktuelle Version zu aktualisieren.

Um von den neuesten Server-Updates zu profitieren, empfiehlt es sich, auf die aktuelle Version von BlackBerry UEM zu aktualisieren.

Bevor Sie beginnen:

- Besuchen Sie BlackBerry myAccount Software Downloads, um die aktuelle Version der BlackBerry Connectivity-App herunterzuladen. Speichern Sie die Dateien auf jedem Computer, der eine UEM-Instanz hostet.
- Weisen Sie die Knox Workspace-Gerätebenutzer an, den BlackBerry UEM Client auf die neueste in Google Play verfügbare Version zu aktualisieren.
- Bei Knox Workspace-Aktivierungen können Benutzer die App selbst aktualisieren, da die neueste Version der BlackBerry Connectivity-App in Google Play verfügbar ist. Sie müssen dennoch die folgenden Schritte ausführen, um UEM für die Unterstützung der App zu konfigurieren.

- Bei Android Enterprise-Aktivierungen können Benutzer selbst über Google Play auf die neueste Version der BlackBerry Connectivity-App aktualisieren, wenn Google Play im geschäftlichen Bereich aktiviert ist. Sie müssen dennoch die folgenden Schritte ausführen, um UEM für die Unterstützung der App zu konfigurieren.
- So konfigurieren Sie UEM für die Unterstützung der BlackBerry Connectivity-App auf Geräten, die BlackBerry Secure Connect Plus erfordern:

1. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Apps**.
2. Klicken Sie auf > **Interne Apps**.
3. Klicken Sie auf **Durchsuchen**, und wählen Sie die .apk-Datei für die neueste BlackBerry Connectivity-App für Android aus.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie im Feld **Senden an** die Option **Alle Android-Geräte** aus.
6. Deaktivieren Sie die Option **App in Google-Domäne veröffentlichen**.
7. Klicken Sie auf **Hinzufügen**.
8. Weisen Sie die App, die Sie im vorherigen Schritt hinzugefügt haben, Samsung Knox Workspace- und Android Enterprise-Geräten zu, die keinen Zugriff auf Google Play haben. Die App-Verfügbarkeit muss auf **Erforderlich** gesetzt sein.

Wenn Sie fertig sind: UEM sendet eine Richtlinien-Aktualisierungsbenachrichtigung an den UEM Client auf Knox Workspace-Geräten. Der UEM Client aktualisiert die BlackBerry Connectivity-App, wenn die App als erforderliche App zugewiesen wird.

Enterprise-Konnektivitätsprofileinstellungen

Enterprise-Konnektivitätsprofile werden auf den folgenden Gerätetypen unterstützt:

- iOS
- iPadOS
- Android

Allgemein: Enterprise-Konnektivitätsprofileinstellungen

Allgemein: Einstellung für Kompatibilitätsprofil	Beschreibung
BlackBerry Secure Connect Plus-Servergruppe	Diese Einstellung gibt die Servergruppe an, die BlackBerry Secure Connect Plus zur Leitung des Datenverkehrs zu einem bestimmten regionalen Pfad verwendet.

iOS: Enterprise-Konnektivitätsprofileinstellungen

Einstellungen für iOS gelten auch für iPadOS-Geräte.

Einstellung	Beschreibung
Enable BlackBerry Secure Connect Plus	Diese Einstellung gibt an, ob geschäftliche Apps BlackBerry Secure Connect Plus für das Senden von geschäftlichen Daten zwischen Geräten und Ihrem Netzwerk verwenden.

Einstellung	Beschreibung
VPN bei Bedarf aktivieren	Wählen Sie diese Einstellung, um nur bestimmten Anwendungen die Nutzung von BlackBerry Secure Connect Plus zu gestatten. **Hinweis:** Wenn Sie diese Option auswählen, müssen Benutzer die VPN-Verbindung für die Verwendung von BlackBerry Secure Connect Plus auf ihren Geräten manuell aktivieren. Solange die VPN-Verbindung aktiv ist, verwendet das Gerät BlackBerry Secure Connect Plus für die Verbindung zum Unternehmensnetzwerk. Die Benutzer müssen die VPN-Verbindung ausschalten, wenn sie eine andere Verbindung, z. B. das Wi-Fi-Unternehmensnetzwerk, verwenden möchten. Weisen Sie die Benutzer an, wenn es angebracht ist, die VPN-Verbindung zu ein- bzw. auszuschalten (die VPN-Verbindung kann beispielsweise aktiviert werden, wenn Benutzer sich nicht im Abdeckungsbereich des geschäftlichen Wi-Fi-Netzwerks aufhalten).
Regeln für „VPN bei Bedarf“ für iOS 9 und höher	Diese Einstellung legt die Verbindungsanforderungen für VPN bei Bedarf mit BlackBerry Secure Connect Plus fest. Sie müssen einen oder mehrere Schlüssel aus dem Beispiel für das Nutzlastformat verwenden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.
Per App VPN aktivieren	Diese Einstellung legt fest, ob geschäftliche Apps automatisch eine VPN-Verbindung mittels BlackBerry Secure Connect Plus starten können, wenn sie Zugriff auf geschäftliche Ressourcen hat. Wählen Sie diese Einstellung, um Regeln für BlackBerry Secure Connect Plus-Verbindungen festzulegen.
Safari-Domänen	Geben Sie die Domänen an, die eine VPN-Verbindung in Safari starten dürfen.
Kalenderdomänen	Legen Sie die Domänen fest, die die VPN-Verbindung im Kalender starten können.
Kontaktdomänen	Legen Sie die Domänen fest, die die VPN-Verbindung in den Kontakten starten können.
E-Mail-Domänen	Legen Sie die Domänen fest, die die VPN-Verbindung im Mailprogramm starten können.
Zugeordnete Domänen	Geben Sie die zugeordneten Domänen an.
Ausgeschlossene Domänen	Geben Sie die ausgeschlossenen Domänen an.
Zulassen, dass Apps automatisch eine Verbindung herstellen	Legen Sie fest, ob Apps die VPN-Verbindung automatisch initiieren können.

Einstellung	Beschreibung
Proxyprofil	Diese Einstellung gibt das zugeordnete Proxy-Profil an, wenn Sie Datenverkehr über einen sicheren Tunnel von Geräten an das geschäftliche Netzwerk über einen Proxyserver leiten wollen. Das Proxy-Profil muss eine manuelle Konfiguration mit einer IP-Adresse verwenden. Die PAC-Konfiguration wird nicht unterstützt. Weitere Informationen finden Sie unter Einrichten von Proxy-Profilen für Geräte.

Android: Enterprise-Konnektivitätsprofileinstellungen

Einstellung	Beschreibung
Enable BlackBerry Secure Connect Plus	Diese Einstellung gibt an, ob geschäftliche Apps BlackBerry Secure Connect Plus für das Senden von geschäftlichen Daten zwischen Geräten und Ihrem Netzwerk verwenden.
Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich	Diese Einstellung gibt an, ob Android Enterprise- und Samsung Knox Workspace-Geräte BlackBerry Secure Connect Plus für alle Apps im geschäftlichen Bereich oder nur für bestimmte Apps verwenden. • „Containerweites VPN“ verwendet eine VPN-Verbindung für alle Apps im geschäftlichen Bereich auf dem Gerät. • „Per App VPN“ verwendet nur für die angegebenen Apps eine VPN-Verbindung.
Apps, die BlackBerry Secure Connect Plus nicht verwenden dürfen	Diese Einstellung gibt Apps im geschäftlichen Bereich auf Android Enterprise-Geräten an, die BlackBerry Secure Connect Plus nicht verwenden dürfen. Wenn die IT-Richtlinienregel „Verwendung von VPN für geschäftliche Anwendungen erzwingen“ auf das Gerät angewendet wird, wird diese Einstellung ignoriert, und geschäftliche Apps, einschließlich BlackBerry UEM Client und Google Play, dürfen BlackBerry Secure Connect Plus nicht verwenden. In diesem Fall müssen Sie Ports in der Firewall öffnen, damit UEM Client mit BlackBerry Infrastructure über UEM kommunizieren kann. Weitere Informationen zum Öffnen von Ports in der Firewall, wenn geschäftliche Apps BlackBerry Secure Connect Plus verwenden, finden Sie unter KB 48330. Wenn Ihr Unternehmen BlackBerry Dynamics-Apps verwendet, wird empfohlen, die Verwendung von BlackBerry Secure Connect Plus durch die Apps einzuschränken. Wenn nicht, müssen Sie zusätzliche Ports in der Firewall Ihres Unternehmens öffnen, damit die Apps Daten an den BlackBerry Dynamics NOC senden können. Die Netzwerkaktivität der Apps ist sonst eventuell verzögert, da die Daten sowohl zur BlackBerry Infrastructure als auch zu BlackBerry Dynamics NOC geleitet werden. Siehe Optimieren von sicheren Tunnelverbindungen für Android-Geräte, die BlackBerry Dynamics-Apps verwenden. Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise -Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Containerweites VPN“ gesetzt ist.

Einstellung	Beschreibung
Apps, die Enterprise-Konnektivität verwenden dürfen	Diese Einstellung gibt Apps im geschäftlichen Bereich auf Android Enterprise- und Samsung Knox Workspace-Geräten an, die BlackBerry Secure Connect Plus verwenden dürfen. Sie können Apps aus einer Liste verfügbarer Apps auswählen oder die App-Paket-ID angeben. Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Per App VPN“ gesetzt ist.
Proxyprofil	Sie können ein Proxy-Profil auswählen, das Sie für die Weiterleitung von sicherem Tunnelverkehr über einen Proxy-Server konfiguriert haben. Diese Option wird für Geräte mit Android Enterprise-Aktivierungsarten unterstützt. BlackBerry Secure Connect Plus unterstützt sowohl die PAC-Konfiguration als auch die manuelle Konfiguration des Proxy-Servers im Proxy-Profil, beachten Sie jedoch die Einschränkungen, die für setHttpProxy von developer.android.com beschrieben sind. Die Web-Proxy-Unterstützung für BlackBerry Secure Connect Plus erfordert die BlackBerry Connectivity-App-Version 1.0.25.x oder höher und UEM Client 12.44.x oder höher.

Festlegen der DNS-Einstellungen für die BlackBerry Connectivity-App

Sie können den DNS-Server festlegen, der von der BlackBerry Connectivity-App für sichere Tunnelverbindungen verwendet werden soll. Wenn Sie keine DNS-Einstellungen festlegen, bezieht die App DNS-Adressen von dem Computer, der die BlackBerry Secure Connect Plus-Komponente hostet, und als standardmäßigen Suchsuffix wird die DNS-Domäne dieses Computers verwendet.

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie bei einer lokalen Umgebung in der UEM-Verwaltungskonsole in der Menüleiste auf **Einstellungen > Infrastruktur > BlackBerry Secure Connect Plus**.
   - Klicken Sie bei einer Cloud-Umgebung in der BlackBerry Connectivity Node-Konsole (http:/localhost:8088) im linken Fensterbereich auf **Allgemeine Einstellungen > BlackBerry Secure Connect Plus**.
2. Aktivieren Sie das Kontrollkästchen **DNS-Server manuell konfigurieren**, und klicken Sie auf +.
3. Geben Sie die Adresse des DNS-Servers in Dezimalschreibweise mit Punkt ein (zum Beispiel: 192.0.2.0). Klicken Sie auf **Hinzufügen**.
4. Wiederholen Sie ggf. die Schritte 2 und 3, um weitere DNS-Server hinzuzufügen. Klicken Sie in der Tabelle **DNS-Server** auf die Pfeile in der Spalte **Rangordnung**, um die Rangordnung der DNS-Server festzulegen.
5. Wenn Sie Suffixe für die DNS-Suche festlegen möchten, führen Sie die folgenden Schritte aus:
   a) Aktivieren Sie das Kontrollkästchen **DNS-Suchsuffixe manuell verwalten**, und klicken Sie auf +.
   b) Geben Sie die das DNS-Suchsuffix ein (z. B. domain.com). Klicken Sie auf **Hinzufügen**.
6. Wiederholen Sie ggf. Schritt 5, um weitere DNS-Suchsuffixe hinzuzufügen. Klicken Sie in der Tabelle **DNS-Suchsuffix** auf die Pfeile in der Spalte **Rangordnung**, um die Rangordnung der DNS-Server festzulegen.
7. Klicken Sie auf **Speichern**.

Optimieren von sicheren Tunnelverbindungen für Android-Geräte, die BlackBerry Dynamics-Apps verwenden

Wenn Sie BlackBerry Secure Connect Plus aktivieren und eine lokale Umgebung mit BlackBerry Dynamics-Apps verwenden, die auf Android Enterprise- oder Samsung Knox Workspace-Geräten installiert sind, sollten Sie die

den Geräten zugewiesenen BlackBerry Dynamics-Konnektivitätsprofile so konfigurieren, dass BlackBerry Proxy deaktiviert ist. Wenn Sie BlackBerry Proxy und BlackBerry Secure Connect Plus gleichzeitig verwenden, wird möglicherweise die Netzwerkaktivität der Apps verzögert, da die Daten an beide Netzwerkkomponenten geleitet werden.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Netzwerke und Verbindungen > BlackBerry Dynamics-Konnektivität**.
2. Bearbeiten Sie das Profil, das Android Enterprise- und Samsung Knox Workspace-Geräten zugewiesen ist.
3. Deaktivieren Sie das Kontrollkästchen **Sämtlichen Datenverkehr weiterleiten**.
4. Wählen Sie im Abschnitt **Standardmäßig zulässiger Domänen-Routingtyp** die Option **Direkt** aus, um den Datenverkehr direkt von der App an die Domäne weiterzuleiten, ohne BlackBerry Proxy zu durchlaufen.
5. Klicken Sie auf **Speichern**.

Fehlerbehebung für BlackBerry Secure Connect Plus

Berücksichtigen Sie die folgenden Aspekte, wenn Sie Probleme mit der Einrichtung von BlackBerry Secure Connect Plus haben.

BlackBerry Secure Connect Plus wird nicht gestartet

Problemursache

Die TCP/IPv4-Einstellungen für den BlackBerry Secure Connect Plus-Adapter sind möglicherweise nicht korrekt.

Mögliche Lösung

Überprüfen Sie unter **Netzwerkverbindungen > BlackBerry Secure Connect Plus Adapter > Eigenschaften > Internet Protocol Version 4 (TCP/IPv4) > Eigenschaften**, ob für **Folgende IP-Adresse verwenden** die folgenden Standardwerte ausgewählt sind:

- IP-Adresse: 172.16.0.1
- Subnetzmaske: 255.255.0.0

Korrigieren Sie diese Einstellungen bei Bedarf, und starten Sie den Server neu.

BlackBerry Secure Connect Plus funktioniert nach der Installation oder einem Upgrade von BlackBerry UEM nicht mehr

Ursache

Dieses Problem kann auftreten, wenn der Server bei einem RRAS-Update nicht neu gestartet wurde, bevor das BlackBerry UEM-Upgrade in einer lokalen Umgebung ausgeführt wurde. Dies führt dazu, dass die NAT-/Routing-Einrichtung während des Upgrades fehlschlägt. Dieses Problem kann auch nach einer Neuinstallation von UEM auftreten.

Lösung

1. Starten Sie den Server neu.
2. Beenden Sie in den Windows-Diensten den Dienst **BlackBerry UEM – BlackBerry Secure Connect Plus**.
3. Starten Sie Windows PowerShell (64-Bit) als Administrator, oder öffnen Sie eine Eingabeaufforderung.
4. Navigieren Sie zu `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\`, und führen Sie **configureRRAS.bat** aus.

5. Navigieren Sie zu `<drive>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\`, und führen Sie **configure-network-interface.cmd** aus.
6. Starten Sie in den Windows-Diensten den Dienst **BlackBerry UEM – BlackBerry Secure Connect Plus**.

Anzeigen der Protokolldateien für BlackBerry Secure Connect Plus

Zweck	Protokoll-datei	Beispiel
Prüfen, ob BlackBerry Secure Connect Plus mit der BlackBerry Infrastructure verbunden ist	BSCP	2015-01-19T13:17:47.540-0500 - BSCP {TcpClientConnectorNio#2} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Received Ping from [id: 0x60bce5a3, /10.90.84.22:28231 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101], responding with Pong.2015-01-19T13:18:22.989-0500 - BSCP {ChannelPinger#1} logging.feature.bscp.service|logging.component.bscp.pss.bcp [{}] - DEBUG Sending Ping to [id: 0xb4a1677a, /10.90.84.22:28232 => stratos.bcp.bblabs.rim.net/206.53.155.152:3101]
Prüfen, ob BlackBerry Secure Connect Plus Aufrufe aus der BlackBerry Connectivity-App auf Geräten empfangen kann	BSCP-TS	47: [14:13:21.231312][][3][AsioTurnSocket-1] Connected, host=68-171-243-141.rdns.blackberry.net 48: [14:13:21.239312][][3][AsioTurnSocket-1] Creating TURN allocation 49: [14:13:21.405121][][3][AsioTurnSocket-1] TURN allocation created
Prüfen, ob Geräte den sicheren Tunnel verwenden	BSCP-TS	74: [10:39:45.746926][][3][Tunnel-2FFEC51E] Sent: 2130.6 KB (1733), Received: 201.9 KB (1370), Running: 00:07:00.139249
Prüfen, ob BlackBerry Secure Connect Plus die benutzerdefinierten Transcodierer-Einstellungen verwendet	BSCP	„configuration_def" : "com.rim.p2e.vpn.server.cipherSuite" }], "TRANSCODER", ["provider", { "configuration_def" : "com.rim.p2e.vpn.transcoder.provider" }, "server_library", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.library" }, "server_config_blob", { "configuration_def" : "com.rim.p2e.vpn.transcoder.server.configBlob" }]]
Prüfen, ob Geräte einen benutzerdefinierten Transcodierer verwenden	BSCP-TS	37: [13:41:39.800371][][3][BlackBerry_1.0.0.1-25B212A5] Connected

Verwenden von BlackBerry 2FA für sichere Verbindungen mit kritischen Ressourcen

BlackBerry 2FA schützt den Zugang zu den kritischen Ressourcen Ihres Unternehmens mithilfe der Zwei-Faktor-Authentifizierung. BlackBerry 2FA verlangt ein Kennwort von Benutzern und zeigt jedes Mal, wenn sie Ressourcen öffnen möchten, eine Sicherheitsaufforderung auf dem Mobilgerät an.

Die Verwaltung von BlackBerry 2FA erfolgt über die BlackBerry UEM-Verwaltungskonsole, in der Sie ein BlackBerry 2FA-Profil zum Aktivieren der Zwei-Faktor-Authentifizierung für Ihre Benutzer verwenden. Um die neueste

Version von BlackBerry 2FA und die zugehörigen Funktionen nutzen zu können, z. B. Vorauthentifizierung und Wiederherstellung, muss den Benutzern das BlackBerry 2FA-Profil zugewiesen werden. Weitere Informationen finden Sie in der Dokumentation zu BlackBerry 2FA.

Aktivieren der automatischen Authentifizierung für iOS-Geräte

Sie können es iOS-Geräten ermöglichen, sich bei Domänen und Webdiensten Ihres Unternehmensnetzwerks automatisch zu authentifizieren. Nach Zuweisung eines Profils oder eines Erweiterungsprofils für die einmalige Anmeldung (Single Sign-On, SSO) wird der Benutzer aufgefordert, beim erstmaligen Zugriff auf eine von Ihnen festgelegte sichere Domäne einen Benutzernamen und ein Kennwort einzugeben. Die Anmeldeinformationen werden auf dem Gerät des Benutzers gespeichert und automatisch verwendet, wenn er versucht, auf die in seinem Profil festgelegten sicheren Domänen zuzugreifen. Wenn der Benutzer das Kennwort ändert, wird er beim nächsten Zugriff auf eine sichere Domäne zur Eingabe aufgefordert.

Sie müssen ein Profil für die SSO-Erweiterung verwenden, damit sich Geräte automatisch bei Domänen und Webservices im Netzwerk Ihres Unternehmens authentifizieren können. Sie können Einstellungen für eine benutzerdefinierte Erweiterung angeben oder die Kerberos-Erweiterung verwenden, die von Apple bereitgestellt wird.

Bevor Sie beginnen: Wenn Sie eine zertifikatbasierte Authentifizierung verwenden möchten, erstellen Sie das erforderliche Profil für das Zertifikat.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Netzwerke und Verbindungen > Single Sign-On-Erweiterung**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie in der Dropdown-Liste **Erweiterungstyp für einmalige Anmeldung** auf **Benutzerdefinierte Erweiterung** oder **Integrierte Kerberos-Erweiterung**, die von Apple bereitgestellt wird.

Aufgabe	Schritte
Wenn Sie **Benutzerdefinierte Erweiterung** auswählen	**a.** Geben Sie im Feld **Erweiterungs-ID** die Kennung für die App ein, die die einmalige Anmeldung durchführt. **b.** Wählen Sie die passende Anmeldeart aus. **c.** Wenn Sie **Anmeldedaten** als Anmeldeart ausgewählt haben, führen Sie die folgenden Schritte aus: **1.** Geben Sie im Feld **Bereich** den Bereichsnamen für die Anmeldedaten ein. **2.** Klicken Sie im Abschnitt **Domänen** auf +, um eine Domäne hinzuzufügen. **3.** Geben Sie im Feld **Name** die Domäne ein, für die die App-Erweiterung die einmalige Anmeldung (Single Sign-On) durchführt. **4.** Fügen Sie nach Bedarf weitere Domänen hinzu. **d.** Wenn Sie als Anmeldeart **Umleiten** ausgewählt haben, führen Sie die folgenden Schritte aus: **1.** Klicken Sie im Abschnitt **URLs** auf +, um eine URL hinzuzufügen. **2.** Geben Sie im Feld **Name** das URL-Präfix des Identitätsanbieters ein, für den die App-Erweiterung die einmalige Anmeldung (Single Sign-On) durchführt. Fügen Sie nach Bedarf weitere URLs hinzu. **e.** Geben Sie im Feld **Benutzerdefinierter Payload-Code** den benutzerdefinierten Payload-Code für die App-Erweiterung ein.

Aufgabe	Schritte
Wenn Sie **Integrierte Kerberos-Erweiterung** auswählen	**a.** Klicken Sie im Abschnitt **Domänen** auf +, um eine Domäne hinzuzufügen. **b.** Geben Sie im Feld **Bereichsname** den Bereichsnamen für die Anmeldedaten ein. **c.** Wählen Sie die entsprechenden **Apple Kerberos SSO-Erweiterungsdaten** für Ihre Umgebung aus. Automatische Anmeldung und Active Directory automatisch erkennen sind standardmäßig zulässig. Sie können auch den Standardbereich angeben, nur verwalteten Apps die Verwendung von Single Sign-On erlauben und den Zugriff durch Benutzer bestätigen lassen. **d.** Legen Sie den **Prinzipalnamen** für die Verbindung fest. **e.** Wenn Sie ein Zertifikatprofil verwenden möchten, um das PKINIT-Zertifikat für die Authentifizierung bereitzustellen, wählen Sie den Profiltyp aus der Dropdown-Liste **PKINIT-Zertifikat für Authentifizierung auswählen** aus, und wählen Sie dann das entsprechende Profil aus. **f.** Wenn Sie die Generic Security Service API verwenden, geben Sie den **GSS-Namen des Kerberos-Cache** an. **g.** Klicken Sie im Abschnitt **App-Bundle-IDs** auf +, um die Bundle-IDs anzugeben, die auf das Ticket Granting Ticket zugreifen können. **h.** Klicken Sie im Abschnitt **Bevorzugte Schlüsselverteilungscenter (KDC)** auf +, um bevorzugte Server anzugeben, wenn sie nicht über DNS erkannt werden können. Geben Sie jeden Server im gleichen Format an, das in der krb5.conf-Datei verwendet wird. Die angegebenen Server werden für Konnektivitätsprüfungen verwendet, wobei zuerst der Kerberos-Datenverkehr getestet wird. Wenn die Server nicht reagieren, verwendet das Gerät die DNS-Erkennung. **i.** Geben Sie im Feld **Benutzerdefinierte Domain-Realm-Zuordnung** alle erforderlichen benutzerdefinierten Zuordnungen von Domänen zu Realm-Namen im Payload-Format ein, z. B. `<key>sample-realm1</key><array><string>org</string></array>`. **j.** Geben Sie im Feld **Anmeldehinweis** den Text an, der unten im Kerberos-Anmeldefenster angezeigt werden soll.

5. Klicken Sie auf **Speichern**.

Angeben des DNS-Servers für iOS- und macOS-Geräte

Sie können die DNS-Server angeben, die Sie für den Zugriff auf bestimmte Domänen verwenden möchten. Diese Einstellung kann Ihnen dabei helfen, das Surfen im Internet schneller und sicherer zu gestalten.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Netzwerke und Verbindungen > DNS**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie auf die Registerkarte eines Gerätetyps.
5. Wählen Sie das DNS-Protokoll für die Kommunikation mit dem DNS-Server aus.
6. Führen Sie einen der folgenden Schritte aus:
   a) Wenn Sie **HTTPS** ausgewählt haben, geben Sie die URI-Vorlage des DNS-over-HTTPS-Servers unter Verwendung des Schemas https:// ein.

b) Wenn Sie **TLS** ausgewählt haben, geben Sie den Hostnamen des DNS-over-TLS-Servers ein.

7. Um zu verhindern, dass Benutzer die Einstellungen deaktivieren, aktivieren Sie das Kontrollkästchen **Nicht zulassen, dass Benutzer DNS-Einstellungen deaktivieren**. Diese Option wirkt sich nur auf überwachte Geräte aus.
8. Geben Sie im Feld **DNS-Adressen** die Liste der IP-Adressen für alle DNS-Server an, die Sie verwenden möchten. Dabei kann es sich um eine Mischung aus IPv4- und IPv6-Adressen handeln.
9. Geben Sie im Feld **Domänen** die Liste der Domänenzeichenfolgen an, die verwendet werden, um zu bestimmen, welche DNS-Abfragen die DNS-Server verwenden.
10. Geben Sie im Feld **Regeln für DNS-On-Demand** die DNS-On-Demand-Regeln mithilfe des Beispiels für das Payload-Format an.
11. Wiederholen Sie die Schritte 5 bis 10 für jeden Gerätetyp.
12. Klicken Sie auf **Speichern**.

Angeben von E-Mail- und Webdomänen für iOS-Geräte

Sie können ein Profil für verwaltete Domänen verwenden, um bestimmte E-Mail-Domänen und Webdomänen als „Verwaltete Domänen“ zu definieren, die intern für Ihr Unternehmen gelten. Profile für verwaltete Domänen gelten nur für iOS- und iPadOS-Geräte mit der Aktivierungsart „MDM-Steuerelemente“.

Nach dem Zuweisen eines Profils für verwaltete Domänen:

- Wenn ein Benutzer eine E-Mail-Nachricht erstellt und eine Empfänger-E-Mail-Adresse mit einer Domäne hinzufügt, die im Profil für verwaltete Domänen nicht angegeben ist, zeigt das Gerät die Adresse in Rot an, um den Benutzer zu warnen, dass es sich um einen externen Empfänger handelt. Das Gerät verhindert nicht, dass der Benutzer E-Mails an externe Empfänger sendet.
- Ein Benutzer muss eine von BlackBerry UEM verwaltete App verwenden, um Dokumente anzuzeigen, die sich auf einer verwalteten Webdomäne befinden oder über eine verwaltete Webdomäne heruntergeladen wurden. Das Gerät verhindert nicht, dass der Benutzer Dokumente auf anderen Webdomänen sucht oder anzeigt. Das Profil für verwaltete Domänen gilt nur für den Safari-Browser.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Netzwerke und Verbindungen > Verwaltete Domänen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
5. Klicken Sie im Abschnitt **Verwaltete Domänen** auf +.
6. Geben Sie im Feld **E-Mail-Domänen** einen Namen für eine Top-Level-Domäne ein (z. B. `example.com` anstelle von `example.com/canada`).
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie im Abschnitt **Verwaltete Webdomänen** auf +. Beispiele für Webdomänenformate finden Sie unter „Managed Safari Web Domains“ in der iOS Developer Library.
9. Geben Sie im Feld **Webdomänen** den Namen einer Domäne ein.
10. Wenn Sie das automatische Ausfüllen von Kennwörtern für die von Ihnen angegebenen Webdomänen zulassen möchten, aktivieren Sie das Kontrollkästchen **Automatisches Ausfüllen des Kennworts zulassen**. Diese Option wird nur für Geräte unter Aufsicht unterstützt.
11. Klicken Sie auf **Hinzufügen** und dann erneut auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie die verwalteten Domänen Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Kontrollieren der Netzwerknutzung von Apps auf iOS-Geräten

Sie können ein Netzwerknutzungsprofil verwenden, um zu steuern, wie die Apps auf iOS- und iPadOS-Geräten das mobile Netzwerk nutzen. Um die Netzwerkauslastung zu steuern, können Sie verhindern, dass die angegebenen Apps Daten übertragen, wenn die Geräte mit dem Mobilfunknetz verbunden sind oder sich im Roaming-Modus befinden. Ein Netzwerknutzungsprofil kann Regeln für eine App oder mehrere Apps enthalten.

Die Regeln in einem Netzwerknutzungsprofil gelten nur für geschäftliche Apps. Wenn Sie keine Apps für Benutzer oder Gruppen zugewiesen haben, hat das Netzwerknutzungsprofil keine Wirkung.

Bevor Sie beginnen: Fügen Sie Apps zur Liste der Apps hinzu, und weisen Sie sie Benutzern und Gruppen zu.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Richtlinien und Profile > Netzwerke und Verbindungen > Netzwerknutzung**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie auf +.
5. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen einer App**, und klicken Sie anschließend auf eine App in der Liste.
   - Wählen Sie die Option **App-Paket-ID angeben** aus, und geben Sie die ID ein. Die App-Paket-ID wird auch als Bundle-ID bezeichnet. Sie können die App-Paket-ID durch Klicken auf die App in der Liste der Apps finden. Verwenden Sie einen Platzhalterwert (*), um die ID mit mehreren Apps abzugleichen. (Z. B. **com.company.***).
6. Um zu verhindern, dass die App oder Apps Daten nutzen, wenn sich das Gerät im Roaming-Modus befindet, deaktivieren Sie das Kontrollkästchen **Datenroaming zulassen**.
7. Um zu verhindern, dass die App oder Apps Daten nutzen, wenn das Gerät mit dem mobilen Netzwerk verbunden ist, deaktivieren Sie das Kontrollkästchen **Mobile Daten zulassen**.
8. Klicken Sie auf **Hinzufügen**.
9. Wiederholen Sie Schritt 5 bis 9 für jede App, die Sie der Liste hinzufügen möchten.

Wenn Sie fertig sind: Wenn Sie mehrere Netzwerknutzungsprofile erstellt haben, weisen Sie ihnen eine Rangordnung zu. Wählen Sie ein Profil aus, und klicken Sie auf ↓↑, um das Profil in der Rangfolge nach oben oder unten zu verschieben. Klicken Sie auf **Speichern**.

Weisen Sie das Netzwerknutzungsprofil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Erstellen von Webinhaltsfilter-Profilen auf iOS-Geräten

Sie können mithilfe von Webinhaltsfilter-Profilen die Webseiten einschränken, die ein Benutzer in Safari oder in anderen Browser-Apps auf einem iOS- oder iPadOS-Gerät unter Aufsicht aufrufen kann. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen Webinhaltsfilter-Profile zuweisen. Wenn Sie ein Webinhaltsfilter-Profil erstellen, muss jede von Ihnen festgelegte URL mit http:// oder https:// beginnen. Ggf. sollten Sie für http:// und https:// separate Eintragsversionen der gleichen URL hinzufügen. Da keine DNS-Auflösung erfolgt, ist es möglich, dass beschränkte Websites nach wie vor aufgerufen werden können (wenn Sie beispielsweise http://www.beispiel.com angeben, könnten die Benutzer dennoch über die IP-Adresse auf die Website zugreifen).

Wenn Sie ein Webinhaltsfilter-Profil erstellen, können Sie die Option der zulässigen Webseiten auswählen, die die Normen Ihrer Organisation in Bezug auf die Nutzung von Mobilgeräten unterstützt.

Zugelassene Websites	Beschreibung
Nur bestimmte Websites	Diese Option erlaubt nur den Zugriff auf die von Ihnen festgelegten Websites. Für jede zugelassene Website wird in Safari ein Lesezeichen erstellt. Wenn Sie den Zugriff nur auf bestimmte Websites zulassen, müssen Sie sicherstellen, dass alle Websites, auf die das Gerät zugreifen muss, in der Liste der zugelassenen Websites angegeben sind. Wenn Sie beispielsweise die moderne Authentifizierung von Microsoft Office 365 für BlackBerry Dynamics-Apps konfigurieren, muss das Gerät die Active Directory Federation Services-Website erreichen können.
Beschränken von nicht jugendfreien Inhalten	Mit dieser Option werden unangemessene Inhalte automatisch erkannt und blockiert. Mit den folgenden Einstellungen können Sie auch bestimmte Websites einbinden: • Erlaubte URLs: Sie können eine oder mehrere URLs hinzufügen, um den Zugriff auf bestimmte Websites zu erlauben. Die Benutzer können die auf dieser Liste aufgeführten Websites unabhängig davon aufrufen, ob die automatische Filterung den Zugriff blockiert. • Gesperrte URLs: Sie können eine oder mehrere URLs hinzufügen, um den Zugriff auf bestimmte Websites zu sperren. Die Benutzer können die auf dieser Liste aufgeführten Websites nicht aufrufen, und zwar unabhängig davon, ob die automatische Filterung den Zugriff erlaubt.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Netzwerke und Verbindungen > Webinhaltsfilter**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Webinhaltsfilter-Profil ein.
4. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Einrichten des Zugriffs auf lediglich bestimmte Websites	a. Vergewissern Sie sich, dass in der Dropdown-Liste **Zugelassene Websites** die Option **Nur bestimmte Websites** ausgewählt ist. b. Klicken Sie im Abschnitt **Lesezeichen für bestimmte Websites** auf +. c. Führen Sie folgende Aktionen aus: 1. Geben Sie im Feld **URL** eine Webadresse ein, für die der Zugriff gestattet werden soll. 2. Optional können Sie auch im Feld **Lesezeichenpfad** den Namen eines Lesezeichen-Ordners eingeben (zum Beispiel: /Work/). 3. Geben Sie im Feld **Titel** einen Namen für die Website ein. 4. Klicken Sie auf **Hinzufügen**. d. Wiederholen Sie für jede zugelassene Website die Schritte b und c.

Aufgabe	Schritte
Beschränken von nicht jugendfreien Inhalten	**a.** Klicken Sie in der Dropdown-Liste **Zugelassene Websites** auf **Nicht jugendfreie Inhalte beschränken**, um die automatische Filterung zu aktivieren. **b.** Führen Sie optional folgende Aktionen aus: 1. Klicken Sie neben **Erlaubte URLs** auf +. 2. Geben Sie eine Webadresse ein, für die der Zugriff gewährt werden soll. 3. Wiederholen Sie den Vorgang bei Bedarf, um weitere Websites zu hinzuzufügen. **c.** Führen Sie optional folgende Aktionen aus: 1. Klicken Sie neben **Gesperrte URLs** auf +. 2. Geben Sie eine Webadresse ein, für die der Zugriff nicht gewährt werden soll. 3. Wiederholen Sie den Vorgang bei Bedarf, um weitere Websites zu hinzuzufügen.

5. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Webinhaltsfilter-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Erstellen eines AirPrint-Profils für iOS-Geräte

Mit den AirPrint-Profilen können Benutzer nach Druckern suchen, die AirPrint unterstützen, die für sie zugänglich sind und für die sie die erforderlichen Berechtigungen besitzen. In Situationen, in denen Protokolle wie BonjourAirPrint-fähige Drucker in einem anderen Subnetzwerk nicht erkennen können, können Sie mithilfe von AirPrint-Profilen angeben, wo sich die entsprechenden Ressourcen befinden. Sie können AirPrint-Profile konfigurieren und iOS- und iPadOS-Geräten zuweisen, damit Benutzer Drucker nicht manuell konfigurieren müssen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Netzwerke und Verbindungen > AirPrint**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie im Abschnitt **AirPrint-Konfiguration** auf +.
5. Geben Sie in das Feld **IP-Adresse** die IP-Adresse für den Drucker oder AirPrint-Server ein.
6. Geben Sie in das Feld **Ressourcenpfad** den Ressourcenpfad des Druckers ein.
   Der Ressourcenpfad des Druckers entspricht dem Parameter `rp` des Bonjour-Datensatzes `_ipps.tcp`.
   Beispiel:
   - Drucker/<*Druckerserie*>
   - Drucker/<*Druckermodell*>
   - ipp/print
   - IPP_Printer
7. Wenn AirPrint-Verbindungen über TLS gesichert werden, aktivieren Sie optional das Kontrollkästchen **TLS erzwingen**.
8. Wenn sich der Port vom Standard für das Internet Printing Protocol unterscheidet, geben Sie optional die Portnummer in das Feld **Port** ein.

9. Klicken Sie auf **Hinzufügen** und dann erneut auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das AirPrint-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Erstellen eines AirPlay-Profils für iOS-Geräte

Bei AirPlay handelt es sich um eine AirPlay-Funktion, mit der Sie Fotos anzeigen oder Musik und Videos auf kompatiblen -Geräten, wie z. B. Apple-TV, Airport Express oder Lautsprecher mit aktiviertem AirPlay, abspielen können.

Mit einem AirPlay-Profil können Sie festlegen, zu welchen AirPlay-Geräten Benutzer von iOS und iPadOS eine Verbindung herstellen können. Das AirPlay-Profil bietet zwei Optionen an:

- Wenn die AirPlay-Geräte Ihres Unternehmens kennwortgeschützt sind, können Sie Gerätekennwörter für zulässige Zielgeräte festlegen, damit Benutzer von iOS- und iPadOS-Geräten eine Verbindung herstellen können, ohne das Kennwort zu kennen.
- Bei überwachten Geräten können Sie einschränken, mit welchen AirPlay-Geräten Benutzer eine Verbindung herstellen können, indem Sie eine Liste der zulässigen AirPlay-Geräte für überwachte Geräte angeben. Überwachte Geräte können nur mit den in der Liste angegebenen AirPlay-Geräten verbunden werden. Wenn Sie keine Liste erstellen, können überwachte Geräte Verbindungen zu jedem beliebigen AirPlay-Gerät herstellen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Netzwerke und Verbindungen > AirPlay**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das AirPlay-Profil ein.
4. Klicken Sie im Abschnitt **Zulässige Zielgeräte** auf +.
5. Geben Sie im Feld **Gerätename** den Namen des AirPlay-Geräts ein, für das Sie das Kennwort bereitstellen möchten. Sie können den Namen des AirPlay-Geräts in den Geräteeinstellungen suchen, oder Sie können den Namen des Geräts durch Tippen auf **Airplay** im Control Center eines iOS- oder iPadOS-Geräts suchen, wodurch eine Liste der verfügbaren AirPlay-Geräte in Ihrer Nähe aufgeführt wird.
6. Geben Sie in das Feld **Kennwort** ein Kennwort ein.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf + im Abschnitt **Zulässige Zielgeräte für Geräte unter Aufsicht**.
9. Geben Sie im Feld **Geräte-ID** die Geräte-ID des AirPlay-Geräts ein, mit dem sich überwachte Geräte verbinden können. Sie können die Geräte-ID für das AirPlay-Gerät in den Geräteeinstellungen finden. Überwachte Geräte können nur mit AirPlay-Geräten in der Liste verbunden werden.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das AirPlay-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Erstellen eines APN-Profils für Android-Geräte

Ein APN (Access Point Name, Zugriffspunktname) gibt die Informationen an, die ein mobiles Gerät benötigt, um eine Verbindung zum Netzwerk eines Netzbetreibers herzustellen. Sie können ein oder mehrere APN-Profile verwenden, um APNs für Betreiber an die Android-Geräte Ihrer Benutzer zu senden. APN-Profile werden von Geräten mit Nur geschäftlicher Bereich-Aktivierungen oder Geschäftlich und persönlich – vollständige Kontrolle-Aktivierungen unterstützt.

In der Regel sind APNs für gängige Betreiber bereits auf den Geräten voreingestellt. Benutzer können einem Gerät auch neue APNs hinzufügen. Wenn Sie ein Gerät zwingen möchten, einen APN zu verwenden, der von

einem APN-Profil an das Gerät gesendet wird, wählen Sie das Kontrollkästchen „Gerät zur Verwendung der APN-Profileinstellungen zwingen“ in der IT-Richtlinienregel aus.

Bevor Sie beginnen: Rufen Sie alle erforderlichen APN-Einstellungen von Ihrem Betreiber ab.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Netzwerke und Verbindungen > Zugriffspunktname**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Diese Informationen werden auf den Geräten angezeigt.
4. Geben Sie im Feld **Zugriffspunktname** den Zugriffspunktnamen ein.
5. Geben Sie die Werte für die jeweilige Profileinstellung entsprechend den Spezifikationen des Betreibers an. Weitere Informationen finden Sie unter Einstellungen für APN-Profil.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Weisen Sie das APN-Profil Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Einstellungen für APN-Profil

Einstellungen für APN-Profil	Beschreibung
Zugriffspunktname	Diese Einstellung legt den APN (Access Point Name) fest, den Ihr Gerät verwenden soll, wenn es mit dem Netzbetreiber kommuniziert. Der APN ist eine kurze Textzeichenfolge.
APN-Bitmaske	Diese Einstellung legt die Datenkommunikationstypen fest, die diese APN-Konfiguration verwenden. Unterschiedliche Datenkommunikationstypen können unterschiedliche Konfigurationen verwenden.
Proxyadresse	Diese Einstellung gibt den HTTP-Proxy an, der für den gesamten Webverkehr über die Verbindung verwendet werden soll. Diese Einstellung ist für die meisten Netzbetreiber nicht erforderlich.
Proxy-Port	Diese Einstellung gibt den HTTP-Proxyport an, der für den gesamten Webverkehr über die Verbindung verwendet werden soll. Diese Einstellung ist für die meisten Netzbetreiber nicht erforderlich.
MMSC	Diese Einstellung legt das Multimedia Messaging Service Center (MMSC) für das Senden und Empfangen von MMS-Nachrichten fest.
MMS-Proxyadresse	Diese Einstellung legt den HTTP-Proxy für die Kommunikation mit dem MMSC zum Senden und Empfangen von MMS-Nachrichten fest.
MMS-Proxyport	Diese Einstellung legt den HTTP-Proxyport für die Kommunikation mit dem MMSC zum Senden und Empfangen von MMS-Nachrichten fest.
Authentifizierungstyp	Diese Einstellung gibt den für die Kommunikation verwendeten Authentifizierungstyp an.
Benutzername	Wenn die Einstellung „Authentifizierungstyp“ auf einen anderen Wert als NONE festgelegt ist, geben Sie einen Benutzernamen an, wenn er für die Authentifizierung erforderlich ist.

Einstellungen für APN-Profil	Beschreibung
Kennwort	Wenn die Einstellung „Authentifizierungstyp“ auf einen anderen Wert als NONE festgelegt ist, geben Sie ein Kennwort an, wenn es für die Authentifizierung erforderlich ist.
Mobile Country Code (MCC)	Diese Einstellung legt den Mobile Country Code für das Netzwerk des Netzbetreibers fest, für das die APN-Konfiguration verwendet werden soll.
Mobile Network Code (MNC)	Diese Einstellung legt den Mobile Network Code für das Netzwerk des Netzbetreibers fest, für das die APN-Konfiguration verwendet werden soll.
Protokoll	Diese Einstellung legt fest, ob IPv4, IPv6 oder beide im Heimnetzwerk für Geräte aktiviert werden sollen, die IPv6-Netzwerke unterstützen.
Roaming-Protokoll	Diese Einstellung legt fest, ob IPv4, IPv6 oder beides beim Roaming für Geräte aktiviert werden soll, die IPv6-Netzwerke unterstützen.
Betreiber-aktiviert	Diese Einstellung legt fest, ob der APN für den Betreiber aktiviert ist.
MVNO-Typ	Diese Einstellung legt fest, ob die Nutzung dieses APN auf bestimmte MVNOs (Mobilfunknetzhändler) oder Abonnentenkonten beschränkt werden soll.

Verwenden von PKI-Zertifikaten mit Geräten oder Apps

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 sicher und 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. Die Zertifizierungsstelle kann das Vertrauen des Zertifikats im Falle eines Verstoßes später widerrufen.

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

- Authentifizieren Sie sich mit SSL/TLS bei der Verbindung mit Webservern, die gegenseitige TLS unterstützen, einschließlich eines geschäftlichen Mailservers.
- 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. BlackBerry UEM bietet eine Reihe von Profilen zur Verwaltung der PKI-Zertifikate auf dem Gerät. Beispiel:

- Vertrauensstellung von Zertifizierungsstellen kann Geräten und Apps mithilfe eines Profils für Zertifizierungsstellenzertifikate zugewiesen werden.
- Die automatische Registrierung von Zertifikaten kann Geräten und Apps über SCEP- und Profile für Benutzeranmeldeinformationen zugewiesen werden.
- Das Abrufen von öffentlichen Verschlüsselungszertifikaten kann Geräten und Apps mithilfe des Zertifikatabrufprofils zugewiesen werden.
- Die Überprüfung des Zertifikatswiderrufstatus kann Geräten und Apps über OCSP- und CRL-Profile zugewiesen werden.

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

Schritt	Aktion
1	Integrieren Sie falls erforderlich 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.

Schritt	Aktion
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 Ihr Unternehmen 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 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 UEM hinzufügen.

Bevor Sie beginnen: Kontaktieren Sie den Entrust-Administrator Ihrer Organisation, um Folgendes zu erhalten:

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

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Einstellungen > Externe Integration > Zertifizierungsstelle**.
2. Klicken Sie auf **Hinzufügen einer Entrust-Verbindung**.
3. Geben Sie im Feld **Verbindungsname** einen Namen für die Verbindung ein.
4. Geben Sie im Feld **URL** die URL für den Entrust MDM Web Service ein.
5. Geben Sie im Feld **Benutzername** den Benutzernamen des Entrust-Administratorkontos ein.
6. Geben Sie im Feld **Kennwort** das Kennwort für das Entrust-Administratorkonto ein.
7. Um ein Zertifizierungsstellenzertifikat hochzuladen, das 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.
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.

Verbinden von BlackBerry UEM mit dem Entrust IdentityGuard-Server Ihres Unternehmens 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 Ihres Unternehmens, 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 der Verwaltungskonsole auf **Einstellungen > Externe Integration > Zertifizierungsstelle**.
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 Ihres Unternehmens

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 > Externe Integration > Zertifizierungsstelle**.
2. Klicken Sie auf **OpenTrust-Verbindung hinzufügen**.
3. Geben Sie im Feld **Verbindungsname** einen Namen für die Verbindung ein.
4. Geben Sie im Feld **URL** die URL für die OpenTrust-Software ein.
5. 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.
6. Geben Sie im Feld **Zertifikatskennwort** das Kennwort für das OpenTrust-Serverzertifikat ein.
7. Um die Verbindung zu testen, klicken Sie auf **Verbindung testen**.
8. 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 UEM-Verbindung mit der OpenTrust-Software zur Verteilung der Zertifikate auf Geräten 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 UEM über die PKI-Verbindung zu verbinden. In einer BlackBerry UEM Cloud-Umgebung muss ein BlackBerry Connectivity Node installiert sein, damit UEM die Kommunikation mit dem PKI-Konnektor über den BlackBerry Cloud Connector möglich ist.

Weitere Informationen über das 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 der Verwaltungskonsole 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 UEM die Authentifizierung mit der BlackBerry Dynamics-PKI-Verbindung mittels kennwortbasierter Authentifizierung durchführt.
   - **Authentifizierung mit Client-Zertifikat**: Wählen Sie diese Option aus, wenn 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 Client-Zertifikat** ausgewählt haben, klicken Sie auf **Durchsuchen**, um ein Zertifikat auszuwählen und hochzuladen, dass von der BlackBerry Dynamics-PKI-Verbindung als vertrauenswürdig eingestuft wird. Geben Sie im Feld **Client-Zertifikatskennwort** das Kennwort für das Zertifikat ein.
8. Im Abschnitt **Vertrauenswürdiges Zertifikat für die PKI-Verbindung** können Sie das Zertifikat angeben, das 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, klicken Sie auf **Durchsuchen**, um zum Zertifizierungsstellenzertifikat Ihres Unternehmens zu navigieren und es auszuwählen.
   - **Serverzertifikat der PKI-Verbindung**: Wenn Sie diese Option auswählen, klicken Sie auf **Durchsuchen**, 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 UEM enthalten ist.

1. Klicken Sie in der Menüleiste der Verwaltungskonsole 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 UEM Client aus, um Purebred verwenden zu können.
4. Klicken Sie auf **Hinzufügen**.

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

- 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 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 UEM herzustellen.	Alle

So wird das Zertifikat hinzugefügt	Beschreibung	Unterstützte Geräte
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
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 macOS (nur für BlackBerry Access) Android Windows 10 (nur für BlackBerry Access)
Profile für freigegebenes Zertifikat	Ein Profil für ein freigegebenes Zertifikat legt ein Clientzertifikat fest, das UEM an iOS-, macOS- und Android-Geräte sendet. 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
Senden von Clientzertifikaten an einzelne Benutzerkonten	Sie können einem Benutzerkonto ein Clientzertifikat hinzufügen. 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

So wird das Zertifikat hinzugefügt	Beschreibung	Unterstützte Geräte
Hochladen von Zertifikaten in UEM Self-Service	Benutzer können Zertifikate in BlackBerry UEM Self-Service hochladen. UEM sendet dann das Zertifikat an die Geräte der Benutzer. 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.	iOS Android
Benutzerimport	Benutzer können dem nativen Schlüsselspeicher des Geräts Zertifikate zur Verwendung mit BlackBerry Dynamics-Apps hinzufügen.	Android

Senden von Clientzertifikaten an Geräte und Apps mithilfe von Profilen

Sie können Zertifikate an Geräte und Apps mithilfe der folgenden Profile senden:

Profil	Beschreibung
Zertifizierungsstellenzertifikat	Profile mit Zertifizierungsstellenzertifikat 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: • Legen Sie fest, wie eine Verbindung zur PKI-Software Ihres Unternehmens hergestellt wird, um Clientzertifikate an Geräte und BlackBerry Dynamics-Apps zu senden. • Laden Sie manuell Zertifikate in BlackBerry UEM hoch, und ermöglichen Sie in einer lokalen Umgebung Benutzern das Hochladen von Zertifikaten mit BlackBerry UEM Self-Service. • Lassen Sie zu, dass BlackBerry Dynamics-Apps auf Android-Geräten und die BlackBerry Access-App auf macOS- und Windows 10-Geräten Zertifikate aus dem nativen Schlüsselspeicher des Geräts verwenden. • Ermöglichen Sie BlackBerry Dynamics-Apps, Zertifikate von anderen App-basierten PKI-Lösungen wie z. B. Purebred zu importieren.

Profil	Beschreibung
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-Dienstes abrufen.
Freigegebenes Zertifikat	Profile für freigegebene Zertifikate legen ein Clientzertifikat fest, das UEM an iOS- und Android-Geräte sendet. 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 und Verwalten eines Client-Zertifikats für ein Benutzerkonto.

Bei iOS- und Android-Geräten 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“ auf dem Bildschirm **App**, Registerkarte **Einstellungen > BlackBerry Dynamics**, für diese App aus.

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 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, VPN und 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.
- Android Enterprise-Geräte unterstützen keine Zertifikate, die über 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 der Verwaltungskonsole auf **Richtlinien und Profile > Zertifikate > Zertifizierungsstellenzertifikat**.
2. Klicken Sie auf +.
3. 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.
4. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
5. 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.
6. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Profil des Zertifizierungsstellenzertifikats Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

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 UEM.
- Eine bestehende Verbindung zwischen 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.

Profile für Benutzeranmeldeinformationen werden auf iOS- und Android-Geräten 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 und Samsung Knox Workspace unterstützt.

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 > Zertifikate > Benutzeranmeldeinformationen**.

2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
4. Wählen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** die Option **Manuell hochgeladenes Zertifikat** aus.
5. Wenn Sie Android Enterprise-Geräte verwalten und Benutzer daran hindern möchten, das Zertifikat für andere Zwecke auszuwählen, wählen Sie auf der Registerkarte **Android** das Kontrollkästchen **Zertifikat auf Android Enterprise-Geräten ausblenden** aus.
6. 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.
- Fügen Sie ein Client-Zertifikat zu einem Profil mit Benutzeranmeldeinformationen hinzu, oder weisen Sie Benutzer an, mit BlackBerry UEM Self-Service ihr eigenes Zertifikat hochzuladen.

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- und Android-Geräte registrieren. Wenn die Verbindung zur Entrust-PKI-Software besteht, kann das Profil für Benutzeranmeldeinformationen auch Zertifikate für BlackBerry Dynamics-Apps registrieren.

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.
- Fragen Sie den Entrust- oder OpenTrust-Administrator nach den Profilwerten, die Sie angeben müssen.
- 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 UEM ein Profil für Benutzeranmeldeinformationen zuweisen, werden die Zertifikate für Benutzer in OpenTrust nicht automatisch erstellt. In diesem Szenario können über das Profil für Benutzeranmeldeinformationen nur Zertifikate an Benutzer verteilt werden, die ein bestehendes Zertifikat im OpenTrust-System aufweisen.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Zertifikate > Benutzeranmeldeinformationen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
4. Wählen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** die von Ihnen konfigurierte Entrust- oder OpenTrust-Verbindung.
5. Klicken Sie in der Dropdown-Liste **Profil** auf das entsprechende Profil.
6. Geben Sie die Werte für das Profil an.
7. 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.

8. Geben Sie den **Erneuerungszeitraum** des Zertifikats ein. Der Zeitraum kann zwischen 1 und 120 Tagen betragen.
9. 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 aufgefordert, das Kennwort einzugeben, das auf dem Bildschirm angezeigt wird.

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.

BlackBerry UEM unterstützt keinen Schlüsselverlauf für abgeleitete Smart Credentials.

Bevor Sie beginnen:

- Verbinden von BlackBerry UEM mit dem Entrust IdentityGuard-Server Ihres Unternehmens 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 > Zertifikate > Benutzeranmeldeinformationen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** auf die Entrust Smart Credential-Verbindung, die Sie konfiguriert haben.
5. 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.
6. 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**, wählen Sie das Kontrollkästchen **An systemeigene Schlüsselkette bereitstellen** aus.

   Wenn diese Einstellung nicht ausgewählt ist, können die Smart Credentials nur von BlackBerry Dynamics-Apps verwendet werden.

7. Wenn die Smart Credentials an BlackBerry Dynamics-Apps gesendet werden, tun Sie auf der Registerkarte **BlackBerry Dynamics** Folgendes:
   a) Wenn Sie die Ablehnung der Zertifikatsanmeldung und späteres Abschließen durch Benutzer zulassen möchten, wählen Sie **Optionale Zertifikatsanmeldung zulassen** aus. Die optionale Zertifikatsanmeldung wird für iOS- und Android-Geräte mit den folgenden Profiltypen für Benutzeranmeldeinformationen unterstützt: Device (App) Based Provider, Entrust Smart Credential und Native Keystore.
   b) Wenn das Gerät doppelte Anmeldedaten löschen soll, wählen Sie **Doppelte Zertifikate löschen**. Das Gerät löscht die Anmeldedaten mit dem frühesten Startdatum.
   c) Wenn das Gerät abgelaufene Anmeldedaten löschen soll, wählen Sie **Abgelaufene Zertifikate löschen**.
   d) Damit alle BlackBerry Dynamics-Apps die Smart Credentials verwenden können, wählen Sie **Allen Apps erlauben, Zertifikate zu verwenden** aus.
   e) 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.
8. 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 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 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 zu verwenden

Sie können das Profil für Benutzeranmeldeinformationen so konfigurieren, dass Zertifikate aus dem nativen Schlüsselspeicher in den folgenden Situationen verwendet werden:

- Zulassen, dass BlackBerry Dynamics-Apps ein Zertifikat aus dem nativen Schlüsselspeicher auf Android-Geräten verwenden.
- Zulassen, dass BlackBerry Dynamics-Apps ein Zertifikat aus dem nativen Schlüsselspeicher verwenden, um auf kryptografische Token von PKI-Apps auf iOS-Geräten zuzugreifen.
- Zulassen, dass die BlackBerry Access-App ein Zertifikat aus dem nativen Schlüsselspeicher auf macOS- oder Windows 10-Geräten verwendet.

Sie können zulassen, dass 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.

Hinweis: „Nativer Schlüsselspeicher“ bezieht sich auf den Schlüsselspeicher auf dem Gerät. Alle Profile für Benutzeranmeldeinformationen mit nativen Schlüsselspeicher-Konnektoren sollten Benutzern zugewiesen werden, bevor sie mit dem Ermitteln von Zertifikaten beginnen. Wenn ein Zertifikat die Anforderungen von mehr als einem UCP erfüllt, wird die beste Übereinstimmung gewählt.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Zertifikate > Benutzeranmeldeinformationen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Profil für ein Zertifizierungsstellenzertifikat muss über einen eindeutigen Namen verfügen.
4. Wählen Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** die Option **Nativer Schlüsselspeicher** aus.

5. Wählen Sie im Abschnitt **Unterstützte Plattformen** die Geräte-OS-Typen aus, die dieses Profil unterstützen soll.
6. Wählen Sie im Abschnitt **Zertifikatsanmeldung** das Kontrollkästchen **Optionale Zertifikatsanmeldung zulassen** aus, wenn Sie Android-Benutzern erlauben möchten, die Zertifikatsanmeldung abzulehnen und sie später abzuschließen.
7. 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, bei denen 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.
8. Wenn das Gerät abgelaufene Zertifikate löschen soll, wählen Sie **Abgelaufene Zertifikate löschen**.
9. Wenn das Gerät doppelte Zertifikate löschen soll, wählen Sie das Kontrollkästchen **Doppeltes Zertifikat entfernen** aus.
10. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Um BlackBerry Dynamics-Apps die Verwendung von Zertifikaten zu gestatten, klicken Sie in der Menüleiste auf **Apps**. Klicken Sie auf die BlackBerry Dynamics-App, die Sie ändern möchten, und wählen Sie dann auf der Registerkarte **Einstellungen > BlackBerry Dynamics** das Kontrollkästchen **BlackBerry Dynamics-Apps die Verwendung von Benutzerzertifikaten, SCEP-Profilen und Benutzeranmeldeprofilen gestatten**.
- 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 > Zertifikate > Benutzeranmeldeinformationen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** auf die von Ihnen konfigurierte BlackBerry Dynamics-PKI-Verbindung.

5. Wenn der Benutzer ein Kennwort zur Anforderung eines Zertifikats angeben muss, wählen Sie **Vom Benutzer eingegebenes Kennwort oder OTP anfordern** aus.
6. 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.
7. Wenn das Gerät abgelaufene Zertifikate löschen soll, wählen Sie das Kontrollkästchen **Abgelaufenes Zertifikat löschen** aus.
8. Wenn das Gerät doppelte Zertifikate löschen soll, wählen Sie das Kontrollkästchen **Doppeltes Zertifikat entfernen** aus.
9. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Um BlackBerry Dynamics-Apps die Verwendung von Zertifikaten zu gestatten, klicken Sie in der Menüleiste auf **Apps**. Klicken Sie auf die BlackBerry Dynamics-App, die Sie ändern möchten, und wählen Sie dann auf der Registerkarte **Einstellungen > BlackBerry Dynamics** das Kontrollkästchen **BlackBerry Dynamics-Apps die Verwendung von Benutzerzertifikaten, SCEP-Profilen und Benutzeranmeldeprofilen gestatten**.
- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.
- Wenn Sie den PKI-Connector aktualisieren, klicken Sie auf **PKI-Funktionen aktualisieren**, um die unterstützten PKI-Funktionen für das Profil zu aktualisieren.
- Wenn Sie die Zertifikate erneuern möchten, die über den PKI-Connector registriert sind, klicken Sie auf **PKI-Funktionen aktualisieren > Erneuern**, um alle BlackBerry Dynamics-fähigen Geräte, die dem Profil zugewiesen sind, anzuweisen, die Zertifikatserneuerung anzufordern.

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 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.

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

Schritt	Aktion
1	Um eine App-basierte 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 den UEM Client für die **Delegierung der App-Authentifizierung** fest.
2	Wenn Sie eine App-basierte PKI-Lösung mit iOS-Geräten verwenden möchten, stellen Sie eine Verbindung zwischen BlackBerry UEM und der App-basierten PKI-Lösung Ihres Unternehmens her.
3	Wenn Sie eine App-basierte PKI-Lösung mit iOS-Geräten verwenden möchten und die PKI-App keine BlackBerry Dynamics-Anwendung ist, konfigurieren Sie BlackBerry UEM Client so, dass App-basierte 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	Verwenden Sie die App-basierte PKI-Lösung mit den folgenden Geräten: • iOS-Geräte: Erstellen eines Profils mit Benutzeranmeldeinformationen zum Verwenden App-basierter Zertifikate. • Android-Geräte: Erstellen eines Profils mit Benutzeranmeldeinformationen, um Zertifikate aus dem nativen Schlüsselspeicher zu verwenden.

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.

Bevor Sie beginnen: Konfigurieren von BlackBerry UEM Client zur Unterstützung von App-basierten Zertifikaten.

1. Klicken Sie in der Menüleiste der UEM-Verwaltungskonsole auf **Apps**.
2. Wählen Sie in der App-Liste den BlackBerry UEM Client aus.
3. Klicken Sie im Abschnitt **App-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 Ihrer Organisation an. Wenn Sie die Purebred-App nutzen, verwenden Sie beispielsweise die folgenden Schemata: `purebred.select.all-user`, `purebred.select.no-filter`, `purebred.zip.all-user`, `purebred.zip.no-filter`.
6. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Weisen Sie 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.

Bevor Sie beginnen: Stellen Sie sicher, dass Sie einen der folgenden Schritte abgeschlossen haben:

- Wenn Ihre Umgebung eine App-basierte PKI-Lösung mit iOS-Geräten verwendet, stellen Sie eine Verbindung zwischen BlackBerry UEM und der App-basierten PKI-Lösung Ihres Unternehmens her.
- Wenn Ihre Umgebung eine App-basierte PKI-Lösung mit iOS-Geräten verwendet und die PKI-App keine BlackBerry Dynamics-App ist, konfigurieren Sie den BlackBerry UEM Client so, dass App-basierte Zertifikate unterstützt werden.

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

Aufgabe	Schritte
Konfigurieren von BlackBerry Work, wenn Ihre Organisation BEMS verwendet	**a.** Aktivieren Sie auf der Registerkarte **Grundlegende Konfiguration** im Abschnitt **Sicherheitseinstellungen** das Kontrollkästchen **Client-Zertifikat anstelle von Anmeldung/Kennwort verwenden**. **b.** Zum Aktivieren der automatischen Erkennung des Microsoft Exchange-Servers, auf dem sich die Benutzer befinden, wählen Sie im Abschnitt **Client-Einstellungen** das Kontrollkästchen **BEMS für die automatische Erkennung des EAS/EWS-Endpunkt des Benutzers verwenden** aus. **c.** Geben Sie auf der Registerkarte **Erweiterte Konfiguration** im Abschnitt **TLS-Zertifikatseinstellungen** den Namen des Profils für Benutzeranmeldeinformationen für das Gerät ein.
Konfigurieren von BlackBerry Work, wenn Ihre Organisation BEMS nicht verwendet	**a.** Klicken Sie auf die Registerkarte **Grundlegende Konfiguration**. **b.** Wenn Ihr Server das Anmeldeformat Domänenname\Benutzer verwendet, geben Sie im Abschnitt **Exchange ActiveSync-Einstellungen** im Feld **Standarddomäne** die Windows NT-Standarddomäne ein, mit der BlackBerry Work eine Verbindung herstellt, wenn sich Benutzer anmelden. **c.** Geben Sie im Feld **Active 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 **Autodiscover-URL** die URL für Autodiscover 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 Abschnitt **TLS-Zertifikatseinstellungen** im Feld **Profilname für die Benutzeranmeldeinformationen** den Namen des Profils für die Benutzeranmeldeinformationen ein.

5. Klicken Sie auf **Speichern**.

Wenn Sie fertig sind: Erstellen Sie eine App-basierte PKI-Lösung zur Verwendung mit den folgenden Geräten:

- iOS-Geräte: Erstellen eines Profils mit Benutzeranmeldeinformationen zum Verwenden App-basierter Zertifikate.
- Android-Geräte: Erstellen eines Profils mit Benutzeranmeldeinformationen, um Zertifikate aus dem nativen Schlüsselspeicher zu verwenden.

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

Bevor Sie beginnen:

- Konfigurieren von BlackBerry UEM Client zur Unterstützung von App-basierten Zertifikaten.
- Stellen Sie sicher, dass die PKI-App (z. B. Purebred) auf den Geräten der Benutzer installiert ist.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile > Zertifikate > Benutzeranmeldeinformationen**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie in der Dropdown-Liste **Zertifizierungsstellenverbindung** auf den Namen der App, 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.
5. 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, bei denen 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
      ```
6. Wenn das Gerät abgelaufene Zertifikate löschen soll, wählen Sie **Abgelaufene Zertifikate löschen**.
7. Wenn das Gerät doppelte Zertifikate löschen soll, wählen Sie **Doppeltes Zertifikat entfernen**.
8. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Um BlackBerry Dynamics-Apps die Verwendung von Zertifikaten zu gestatten, klicken Sie in der Menüleiste auf **Apps**. Klicken Sie auf die BlackBerry Dynamics-App, die Sie ändern möchten, und wählen Sie dann auf der Registerkarte **Einstellungen > BlackBerry Dynamics** das Kontrollkästchen **BlackBerry Dynamics-Apps die Verwendung von Benutzerzertifikaten, SCEP-Profilen und Benutzeranmeldeprofilen gestatten**.
- 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 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 > Zertifikate > SCEP**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. 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. Beachten Sie, dass die folgenden Einstellungen im SCEP-Profil nicht für folgende OpenTrust-Clientzertifikate gelten: 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.
5. 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.

6. Geben Sie im Feld **Instanzname** den Instanznamen der Zertifizierungsstelle ein.
7. Deaktivieren Sie optional das Kontrollkästchen für alle Gerätetypen, für die Sie das Profil nicht konfigurieren möchten.
8. 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. Siehe:
      - Allgemein: SCEP-Profileinstellungen
      - iOS: SCEP-Profileinstellungen
      - macOS: SCEP-Profileinstellungen
      - Android: SCEP-Profileinstellungen
      - Windows 10: SCEP-Profileinstellungen
      - BlackBerry Dynamics: SCEP-Profileinstellungen
9. Wiederholen Sie Schritt 8 für jeden Gerätetyp in Ihrer Organisation.
10. 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.

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.
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 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 UEM-Zertifikatspeicher nach der Stammzertifizierungsstelle des SCEP-Servers sucht, um für 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.

Allgemein: SCEP-Profileinstellung	Beschreibung
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. Für Windows-Geräte werden nur „statische“ Kennwörter unterstützt.
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. 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.
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. 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 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 Variablen wie „%UserDistinguishedName%“.
Wiederholungen	Diese Einstellung legt fest, wie oft der Verbindungsaufbau zum SCEP-Dienst wiederholt wird, wenn der erste Verbindungsversuch fehlgeschlagen ist.
Wiederholungsverzögerung	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest.
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.
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.

iOS: SCEP-Profileinstellung	Beschreibung
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.

macOS: SCEP-Profileinstellungen

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.
Profil anwenden auf	Diese Einstellung gibt an, ob das SCEP-Profil für das Benutzerkonto oder das Gerät gilt.
Empfänger	Diese Einstellung legt den Betreff für das Zertifikat fest, falls dieser für die SCEP-Konfiguration Ihrer Organisation erforderlich ist. Geben Sie den Betreff im Format „/CN=<*common_name*>/O=<*domain_name*>“ ein. Wenn das Profil für mehrere Benutzer bestimmt ist, können Sie eine Variable verwenden, z. B. %UserDistinguishedName%.
Wiederholungen	Diese Einstellung legt fest, wie oft der Verbindungsaufbau zum SCEP-Dienst wiederholt wird, wenn der erste Verbindungsversuch fehlgeschlagen ist.
Wiederholungsverzögerung	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest.
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.

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

Informationen zu Geräten mit Android Management-Aktivierungsarten finden Sie unter Überlegungen zu Aktivierungsarten für Android Management.

Android: SCEP-Profileinstellung	Beschreibung
BlackBerry UEM als Proxy für SCEP-Anforderungen verwenden	Diese Einstellung legt fest, ob alle SCEP-Anforderungen von Geräten per 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 gibt an, ob das Zertifikat für Android Enterprise-Benutzer 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 UEM Cloud angezeigt.
Verschlüsselungsalgorithm	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, den Android-Geräte für die Zertifikatsanmeldungsanforderung verwenden.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die Android-Geräte für die Zertifikatsanmeldungsanforderung verwenden.
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.

Android: SCEP-Profileinstellung	Beschreibung
Automatische Erneuerung	Diese Einstellung legt fest, wie viele Tage vor Ablauf eines Zertifikats diese automatische Zertifikatserneuerung erfolgen soll.
Android-Arbeitsprofile und 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 Variablen wie „%UserDistinguishedName%“.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest.
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 Geräte verwenden, um das Client-Schlüsselpaar zu generieren. Sie müssen einen Algorithmus auswählen, der von Ihrer Zertifizierungsstelle unterstützt wird.
RSA-Stärke	Diese Einstellung legt die RSA-Stärke fest, die 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.
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können.
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an.

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.

Windows 10: 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 Variablen wie „%UserDistinguishedName%“.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest.
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.
Wiederholungsverzögerung	Diese Einstellung legt fest, wie viele Sekunden bis zum nächsten Versuch, eine Verbindung zum SCEP-Dienst aufzubauen, verstreichen sollen.
Schlüsselgröße	Diese Einstellung legt die Schlüsselgröße für das Zertifikat fest.
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können.
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an.
SCEP-Schlüsselspeicher	Diese Einstellung gibt den Speicherort für den privaten Schlüssel an.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die ein Windows 10-Gerät für die Zertifikatsanmeldungsanforderung verwendet.
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. Der Höchstwert beträgt 365 Tage.

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 Variablen wie „%UserDistinguishedName%“.
SAN-Typ	Diese Einstellung legt ggf. den Alternativnamen des Zertifikatempfängers für das Zertifikat fest.
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.
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.
Verschlüsselungsalgorithm	Diese Einstellung legt den Verschlüsselungsalgorithmus fest, der für die Zertifikatsanmeldungsanforderung verwendet wird.
Hashfunktion	Diese Einstellung legt die Hashfunktion fest, die für die Zertifikatsanmeldungsanforderung verwendet wird.
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.
Schlüsselnutzung	Diese Einstellung gibt die kryptografischen Vorgänge an, die mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels ausgeführt werden können.

BlackBerry Dynamics: SCEP-Profileinstellung	Beschreibung
Erweiterte Schlüsselnutzung	Diese Einstellung gibt den Zweck des im Zertifikat enthaltenen Schlüssels an.
App-Einschränkungen	Diese Einstellung gibt an, welche BlackBerry Dynamics-Apps das Zertifikat verwenden können.
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.

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 > Zertifikate > Freigegebenes Zertifikat**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Geben Sie im Feld **Kennwort** ein Kennwort für das Profil des freigegebenen Zertifikats ein.
5. Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**, um die Zertifikatsdatei zu finden.
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.
7. Wenn Sie macOS-Geräte verwalten, wählen Sie auf der Registerkarte **macOS** in der Dropdown-Liste **Profil anwenden auf** den Eintrag **Benutzer** oder **Gerät** aus.
8. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind: Weisen Sie das Profil für freigegebenes Zertifikat Benutzerkonten, Benutzergruppen oder Gerätegruppen zu.

Angeben des Zertifikats, das von einer App mit einem Zertifikatzuordnungsprofil verwendet wird

Bei Android-Geräten 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.

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 > Zertifikate > Zertifikatzuordnung**.
2. Klicken Sie auf +.
3. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
4. Klicken Sie in der Zuordnungstabelle auf +.
5. 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.
6. 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** aus, und klicken Sie auf den Profilnamen aus der Dropdown-Liste.
   - 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.
   - Um anzugeben, dass die App ein Zertifikat verwenden muss, das über ein anderes Profil an das Gerät gesendet wird, wählen Sie **Ausgewähltes Zertifikat** aus, und klicken Sie auf den Profilnamen aus der Dropdown-Liste.
7. 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.
8. Wiederholen Sie bei Bedarf die Schritte 5 bis 8, um zusätzliche Zuordnungen zu dem Profil hinzuzufügen.
9. Klicken Sie auf **Hinzufügen**.

Wenn Sie fertig sind:

- Weisen Sie die Profile Benutzerkonten und Benutzergruppen zu.
- Wenn Sie mehr als ein Zertifikatzuordnungsprofil erstellen möchten, dann legen Sie nach Bedarf eine Rangfolge für die Profile fest. Wählen Sie ein Profil aus, und klicken Sie auf ↓↑, um das Profil in der Rangfolge nach oben oder unten zu verschieben. Klicken Sie auf **Speichern**.

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 für andere verwaltete iOS- und Android-Geräte unterstützt. Das Hochladen von Zertifikaten in Profile für Benutzeranmeldeinformationen wird für 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 und Verwalten eines Client-Zertifikats für ein Benutzerkonto

1. Klicken Sie in der Menüleiste der Verwaltungskonsole auf **Benutzer > Verwaltete Geräte**.
2. Suchen Sie nach einem Benutzerkonto, und klicken Sie darauf.
3. Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Schritte
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. **a.** Klicken Sie im Abschnitt **IT-Richtlinie und -Profile** auf +. **b.** Klicken Sie auf **Benutzerzertifikat**. **c.** Geben Sie eine Beschreibung für das Zertifikat ein. **d.** Wählen Sie im Abschnitt **Zertifikat anwenden auf** eine der folgenden Optionen aus: 1. **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. 2. **BlackBerry Dynamics-fähige Geräte**: Wählen Sie diese Option aus, um das Zertifikat zur Verwendung mit BlackBerry Dynamics-Apps an Geräte zu senden. **e.** Klicken Sie im Feld **Zertifikatsdatei** auf **Durchsuchen**. Navigieren Sie zu der Zertifikatsdatei, und wählen Sie sie aus. **f.** Wenn Sie **Andere verwaltete Geräte** aktivieren, geben Sie ein Kennwort für das Zertifikat in das Feld **Kennwort** ein. Für iOS-Geräte ist ein Kennwort erforderlich. Bei Android-Geräten muss kein Kennwort festgelegt werden, wenn auf dem Gerät die aktuelle Version des UEM Client ausgeführt wird. Wenn Sie kein Kennwort festlegen, muss der Benutzer das Gerätekennwort eingeben. **g.** Klicken Sie auf **Hinzufügen**. **h.** Konfigurieren der Gültigkeitsdauer für Clientzertifikate. Die standardmäßige Gültigkeitsdauer bis zum Entfernen der Client-Zertifikate beträgt 24 Stunden. 1. Klicken Sie in der Menüleiste auf **Einstellungen > Allgemeine Einstellungen > Zertifikate**. 2. Legen Sie die Gültigkeitsdauer für PKCS12-Zertifikate auf dem Server fest.

Aufgabe	Schritte
Erneuern oder Entfernen eines BlackBerry Dynamics-Zertifikats für ein Benutzerkonto	Sie können einen Befehl an das Gerät eines Benutzers senden, um die Zertifikatsverlängerung von der Zertifizierungsstelle anzufordern. Sie können auch ein BlackBerry Dynamics-Zertifikat vom Gerät eines Benutzers entfernen. Wenn Sie ein Zertifikat entfernen, sendet der BlackBerry Dynamics-PKI-Connector eine Benachrichtigung an die Zertifizierungsstelle, dass das Zertifikat nicht mehr verwendet, aber nicht automatisch gesperrt wird. Führen Sie im Abschnitt **Benutzerzertifikate** eine der folgenden Aktionen aus: **a.** Klicken Sie zum Anfordern einer Zertifikaterneuerung von der Zertifizierungsstelle auf ⟳. **b.** Klicken Sie zum Entfernen des Zertifikats vom Gerät des Benutzers auf ✕. Um eine Entrust Smart Credential von einem Gerät zu entfernen, muss der Benutzer die Smart Credential auch im BlackBerry UEM Client deaktivieren.
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 UEM Self-Service in das entsprechende Profil hochladen. Das Hochladen von Zertifikaten in Profile für Benutzeranmeldeinformationen wird für 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 anfangen:** • Profil mit Benutzeranmeldeinformationen zum manuellen Hochladen von Zertifikaten erstellen. • Weisen Sie Benutzern das Profil mit Anmeldeinformationen zu. **a.** Klicken Sie im Abschnitt **IT-Richtlinie und -Profile** neben dem Profil für Benutzeranmeldeinformationen auf **Ein Zertifikat hinzufügen**. **b.** Klicken Sie auf **Durchsuchen**. Navigieren Sie zu dem Zertifikat, und wählen Sie es aus. **c.** Geben Sie das Kennwort für das Zertifikat ein. Für iOS-Geräte ist das Kennwort erforderlich. Bei Android-Geräten muss das Kennwort in UEM nicht angegeben werden, wenn auf dem Gerät die aktuelle Version des UEM Client ausgeführt wird. Wenn Sie das Kennwort nicht festlegen, muss der Benutzer das Gerätekennwort eingeben. **d.** Klicken Sie auf **Hinzufügen**.

Aufgabe	Schritte
Hinzufügen eines Client-Zertifikats für ein Profil mit Benutzeranmeldeinformationen	Das neue Zertifikat ersetzt das auf dem Gerät vorhandene Zertifikat. **a.** Klicken Sie im Abschnitt **IT-Richtlinie und -Profile** neben dem Profil für Benutzeranmeldeinformationen auf **Aktualisieren**. **b.** Klicken Sie auf **Durchsuchen**, um zum Speicherort des Zertifikats zu gehen. **c.** Geben Sie das Kennwort für das Zertifikat ein. Für iOS-Geräte ist das Kennwort erforderlich. Für Android-Geräte muss das Kennwort in UEM nicht angegeben werden, wenn auf dem Gerät die aktuelle Version von UEM Client ausgeführt wird. Wenn Sie das Kennwort nicht festlegen, muss der Benutzer das Gerätekennwort eingeben. **d.** Klicken Sie auf **Speichern**.

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada