



# **BlackBerry UEM**

## **Schützen von Netzwerkverbindungen**

Verwalten

12.13



# Inhalt

<b>Verwalten von Wi-Fi-, VPN-, BlackBerry Secure Connect Plus und anderen geschäftlichen Verbindungen.....</b>	<b>5</b>
<b>Verwalten von geschäftlichen Verbindungen mithilfe von Profilen.....</b>	<b>6</b>
<b>Bewährtes Verfahren: Erstellen von Profilen für Geschäftsverbindungen.....</b>	<b>7</b>
<b>Einrichten von geschäftlichen Wi-Fi-Netzwerken für Geräte.....</b>	<b>8</b>
Erstellen eines Wi-Fi-Profiles.....	8
Wi-Fi-Profileinstellungen.....	9
Allgemein: Wi-Fi-Profileinstellungen.....	9
iOS und macOS: Wi-Fi-Profileinstellungen.....	9
Android: Wi-Fi-Profileinstellungen.....	16
Windows: Wi-Fi-Profileinstellungen.....	21
BlackBerry 10: Wi-Fi-Profileinstellungen.....	26
<b>Einrichten von geschäftlichen VPNs für Geräte.....</b>	<b>32</b>
Erstellen eines VPN-Profiles.....	33
VPN-Profileinstellungen.....	33
iOS und macOS: VPN-Profileinstellungen.....	33
Android: VPN-Profileinstellungen.....	43
Windows 10: VPN-Profileinstellungen .....	49
BlackBerry 10: VPN-Profileinstellungen.....	55
Per App VPN aktivieren.....	71
So wählt BlackBerry UEM die Per App VPN-Einstellungen für die Zuweisung zu iOS-Geräten aus.....	71
<b>Einrichten von Proxy-Profilen für Geräte.....</b>	<b>73</b>
Erstellen eines Proxy-Profiles.....	74
<b>Verwenden von BlackBerry Secure Connect Plus für Verbindungen mit geschäftlichen Ressourcen.....</b>	<b>76</b>
Schritte zum Aktivieren von BlackBerry Secure Connect Plus.....	76
Server- und Geräteanforderungen für BlackBerry Secure Connect Plus.....	77
Installieren zusätzlicher BlackBerry Secure Connect Plus-Komponenten in einer lokalen Umgebung.....	78
Installieren oder Aktualisieren der BlackBerry Secure Connect Plus-Komponente in einer Cloud-Umgebung.....	79
BlackBerry Secure Connect Plus aktivieren.....	79
Enterprise-Konnektivitätsprofileinstellungen.....	80
Festlegen der DNS-Einstellungen für die BlackBerry Connectivity-App.....	83

Optimieren von sicheren Tunnelverbindungen für Android-Geräte, die BlackBerry Dynamics-Apps verwenden.....	84
Leiten des geschäftlichen Datenverkehrs in BlackBerry 10 über BlackBerry Secure Connect Plus, wenn ein Wi-Fi-Netzwerk verfügbar ist.....	84
Fehlerbehebung für BlackBerry Secure Connect Plus.....	85
BlackBerry Secure Connect Plus-Adapter wechselt in den Zustand „Nicht identifiziertes Netzwerk“ und funktioniert nicht mehr.....	85
BlackBerry Secure Connect Plus wird nicht gestartet.....	86
BlackBerry Secure Connect Plus funktioniert nach der Installation oder einem Upgrade von BlackBerry UEM nicht mehr.....	86
Anzeigen der Protokolldateien für BlackBerry Secure Connect Plus.....	87
<b>Verwenden der Enterprise-Konnektivität für BlackBerry 10-Geräte.....</b>	<b>88</b>
Verwaltung der Enterprise-Konnektivität für BlackBerry 10-Geräte.....	88
<b>Verwenden von BlackBerry 2FA für sichere Verbindungen mit kritischen Ressourcen.....</b>	<b>89</b>
<b>Einrichten einer Authentifizierung bei einmaliger Anmeldung für Geräte.....</b>	<b>90</b>
Voraussetzungen: Verwenden der Kerberos-Authentifizierung für Geräte.....	90
Zertifikatbasierte Authentifizierung für iOS-Geräte.....	91
Erstellen eines Profils für die einmalige Anmeldung.....	91
SSO-Erweiterungsprofil erstellen.....	93
<b>Verwalten von E-Mail- und Webdomänen für iOS-Geräte.....</b>	<b>95</b>
Erstellen eines Profils für verwaltete Domänen.....	95
<b>Kontrollieren der Netzwerknutzung von Apps auf iOS-Geräten.....</b>	<b>96</b>
Erstellen eines Netzwerknutzungsprofils.....	96
<b>Filtern von Webinhalten auf iOS-Geräten.....</b>	<b>97</b>
Erstellen von Webinhaltsfilter-Profilen.....	97
<b>Konfigurieren von AirPrint- und AirPlay-Profilen für iOS-Geräte.....</b>	<b>99</b>
Erstellen eines AirPrint-Profiles.....	99
Erstellen eines AirPlay-Profiles.....	100
<b>Konfigurieren von Zugriffspunktnamen für Android-Geräte.....</b>	<b>101</b>
Erstellen eines APN-Profiles.....	101
Einstellungen für APN-Profil.....	101
<b>Rechtliche Hinweise.....</b>	<b>104</b>

# Verwalten von Wi-Fi-, VPN-, BlackBerry Secure Connect Plus und anderen geschäftlichen Verbindungen

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-, Windows- und BlackBerry 10-Geräte in dem gleichen Profil festlegen und das Profil dann Benutzerkonten, Benutzergruppen oder Gerätegruppen zuweisen.

# Verwalten von geschäftlichen Verbindungen mithilfe von Profilen

Sie können mithilfe der folgenden Profile, die in der Bibliothek „Richtlinien und Profile“ verfügbar sind, konfigurieren, wie Geräte eine Verbindung zu Arbeitsressourcen herstellen.

Profil	Beschreibung
Wi-Fi	Ein Wi-Fi-Profil legt fest, wie die Geräte eine Verbindung zu einem geschäftlichen Wi-Fi-Netzwerk aufbauen.
VPN	Ein VPN-Profil legt fest, wie die Geräte eine Verbindung zu einem geschäftlichen VPN aufbauen.
Proxy	Ein Proxy-Profil legt fest, wie die Geräte einen Proxy-Server nutzen, um auf Webdienste im Internet oder auf ein geschäftliches Netzwerk zuzugreifen.
Enterprise-Konnektivität	<p>Das Enterprise-Konnektivitätsprofil legt fest, wie Geräte mithilfe der Enterprise-Konnektivität und BlackBerry Secure Connect Plus eine Verbindung zu den Ressourcen Ihres Unternehmens herstellen können.</p> <p>iOS-, Android Enterprise-, Samsung Knox Workspace und BlackBerry 10-Geräte können mit BlackBerry Secure Connect Plus sichere Verbindungen zu geschäftlichen Ressourcen hinter der Firewall herstellen.</p>
BlackBerry 2FA	Ein BlackBerry 2FA-Profil ermöglicht den Einsatz der Zwei-Faktor-Authentifizierung für Benutzer und legt die Konfiguration der Funktionen für die Vorauthentifizierung und Wiederherstellung fest.
Einmalige Anmeldung	Ein Profil für die einmalige Anmeldung legt fest, wie die Geräte bei sicheren Domänen automatisch eine Authentifizierung durchführen, nachdem die Benutzer zum ersten Mal ihren Benutzernamen und ihr Kennwort eingegeben haben.
BlackBerry Dynamics-Konnektivitätsprofil	Ein BlackBerry Dynamics-Konnektivitätsprofil definiert die Netzwerkverbindungen, Internetdomänen, IP-Adressbereiche und App-Server, zu denen Geräte mithilfe von BlackBerry Dynamics-Apps eine Verbindung herstellen können.
E-Mail	E-Mail-Profile legen fest, 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.
IMAP/POP3-E-Mail	Ein IMAP/POP3-E-Mail-Profil legt fest, wie Geräte eine Verbindung mit einem IMAP- bzw. POP3-E-Mail-Server aufbauen und E-Mail-Nachrichten synchronisieren.

# Bewährtes Verfahren: Erstellen von Profilen für Geschäftsverbindungen

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.

Beachten Sie die folgenden Richtlinien:

- Legen Sie fest, welche geschäftlichen Verbindungen für die Geräte in Ihrer Organisation erforderlich sind.
- Erstellen Sie Profile, die Sie mit anderen Profilen verknüpfen können, bevor Sie die Verbindungsprofile erstellen, die diese Profile nutzen.
- Verwenden Sie wenn möglich Variablen.

Sie können 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-Profil 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 die auf dem Gerät gespeicherten Wi-Fi-Profil verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen.

## Erstellen eines Wi-Fi-Profiles

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen vom Wi-Fi-Sicherheitstyp und dem Authentifizierungsprotokoll ab, die Sie ausgewählt haben.

### Bevor Sie beginnen:

- Wenn die Geräte eine zertifikatbasierte Authentifizierung für geschäftliche Wi-Fi-Verbindungen 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 Benutzeranmeldeinformationen oder ein Profil für ein freigegebenes Zertifikat, das Sie mit dem Wi-Fi-Profil verknüpfen.  
**Hinweis:** Samsung Knox Workspace-Geräte unterstützen keine Zertifikate, die über BlackBerry UEM zur WLAN-Authentifizierung an Geräte gesendet werden. Benutzer müssen die zertifikatbasierte Authentifizierung auf Samsung Knox Workspace-Geräten manuell einrichten.
  - Bei BlackBerry 10-, iOS-, macOS-, Android Enterprise- und Samsung Knox-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.
  - Wenn BlackBerry 10-Geräte ein VPN für geschäftliche Wi-Fi-Verbindungen verwenden, erstellen Sie ein VPN-Profil, das Sie mit dem Wi-Fi-Profil verknüpfen.
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. 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 Wi-Fi-Konfiguration in Ihrer Unternehmensumgebung entsprechen. Wenn Ihr Unternehmen erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für den Zugriff auf das Wi-Fi-Netzwerk eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername** %UserName% ein.
  8. Wiederholen Sie Schritt 7 für jeden Gerätetyp in Ihrer Organisation.
  9. Klicken Sie auf **Hinzufügen**.



# Wi-Fi-Profileinstellungen

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. [Wi-Fi-Profile](#) werden auf den folgenden Gerätetypen unterstützt:

- iOS
- macOS
- Android
- Windows
- BlackBerry 10

## Allgemein: Wi-Fi-Profileinstellungen

Allgemein: Wi-Fi-Profileinstellung	Beschreibung
SSID	Diese Einstellung gibt den Netzwerknamen eines Wi-Fi-Netzwerks und seiner drahtlosen Zugriffspunkte an. Bei der SSID muss die Groß- und Kleinschreibung beachtet werden, und sie muss alphanumerische Zeichen enthalten.  Mögliche Werte sind auf 32 Zeichen begrenzt.
Verborgenes Netzwerk	Diese Einstellung legt fest, ob die SSID im Wi-Fi-Netzwerk verborgen ist.

## iOS und macOS: Wi-Fi-Profileinstellungen

Bei macOS gelten Profile für Benutzerkonten oder Geräte. Sie können ein Wi-Fi-Profil konfigurieren, das für Benutzerkonten oder Geräte gilt.

iOS 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.  Mögliche Werte: <ul style="list-style-type: none"><li>• Benutzer</li><li>• Gerät</li></ul> Diese Einstellung ist nur für macOS gültig.
Automatisch dem Netzwerk beitreten	Diese Einstellung gibt an, ob ein Gerät automatisch dem Wi-Fi-Netzwerk hinzugefügt werden kann.
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.

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Netzwerktyp	<p>Diese Einstellung legt eine Konfiguration für das Wi-Fi-Netzwerk fest.</p> <p>Hotspot-Konfigurationen stehen nur für iOS- und macOS-Geräte zur Verfügung. Um Wi-Fi-Einstellungen für Android- und BlackBerry 10-Geräte zu konfigurieren, müssen Sie ein separates Wi-Fi-Profil erstellen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Legacy-Hotspot</li> <li>• Hotspot 2.0</li> </ul> <p>Der Standardwert ist „Standard“.</p>
Angezeigter Betreibername	<p>Diese Einstellung legt den Anzeigenamen des Hotspot-Betreibers fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.</p>
Domänenname	<p>Diese Einstellung legt den Domännennamen des Hotspot-Betreibers fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.</p> <p>Wenn Sie diese Einstellung verwenden, ist die Einstellung „SSID“ nicht erforderlich.</p>
Unternehmensbezeichner der Roaming-Konsortien	<p>Diese Einstellung legt die Organisationsbezeichner der Roaming-Konsortien und Dienstanbieter fest, auf die über den Hotspot zugegriffen werden kann.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.</p>
NAI-Bereichsnamen	<p>Diese Einstellung legt die NAI-Bereichsnamen fest, die ein iOS-Gerät authentifizieren können.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.</p>
MCC/MNCs	<p>Diese Einstellung legt die MCC/MNC-Kombinationen fest, die Mobilfunknetzbetreiber identifizieren. Jeder Wert muss genau sechs Ziffern umfassen.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.</p>
Verbindungsaufbau zu Roaming-Partnernetzwerken zulassen	<p>Diese Einstellung legt fest, ob ein Gerät eine Verbindung zu Roaming-Partnern für den Hotspot aufbauen kann.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.</p>

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Sicherheitstyp	<p>Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet.</p> <p>Wenn die Einstellung „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist, ist diese Einstellung auf „WPA2-Enterprise“ gesetzt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• WEP persönlich</li> <li>• WEP Unternehmen</li> <li>• WPA-Personal</li> <li>• WPA-Enterprise</li> <li>• WPA2-Personal</li> <li>• WPA2-Enterprise</li> <li>• WPA3-Personal</li> <li>• WPA3-Enterprise</li> </ul> <p>Der Standardwert ist „Keine“.</p>
WEP-Schlüssel	<p>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.</p> <p>Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.</p>
Preshared key	<p>Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“, „WPA2-Personal“ oder „WPA3-Personal“ gesetzt ist.</p>
<b>Protokolle</b>	
Authentifizierungsprotokoll	<p>Diese Einstellung legt die EAP-Methoden fest, die das Wi-Fi-Netzwerk unterstützt. Sie können mehrere EAP-Methoden auswählen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „WPA3-Enterprise“ gesetzt ist.</p> <p>Mögliche Auswahlen:</p> <ul style="list-style-type: none"> <li>• TLS</li> <li>• TTLS</li> <li>• LEAP</li> <li>• PEAP</li> <li>• EAP-FAST</li> <li>• EAP-SIM</li> </ul>

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Interne Authentifizierung	<p>Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• PAP</li> <li>• CHAP</li> <li>• MS-CHAP</li> <li>• MS-CHAPv2</li> <li>• EAP</li> </ul> <p>Der Standardwert ist „MS-CHAPv2“.</p>
PAC verwenden	<p>Diese Einstellung legt fest, ob die EAP-FAST-Methode geschützte Anmeldeinformationen (Protected Access Credential) verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist.</p>
PAC bereitstellen	<p>Diese Einstellung legt fest, ob die EAP-FAST-Methode die Bereitstellung von geschützten Anmeldeinformationen zulässt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt und die Einstellung „PAC verwenden“ ausgewählt ist.</p>
PAC anonym bereitstellen	<p>Diese Einstellung legt fest, ob die EAP-FAST-Methode die anonyme Bereitstellung von geschützten Anmeldeinformationen zulässt.</p> <p>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.</p>
<b>Authentifizierung</b>	
Externe Identität für TTLS, PEAP und EAP-FAST	<p>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“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“, „PEAP“ oder „EAP-FAST“ gesetzt ist.</p>

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Im Wi-Fi-Profil enthaltenes Kennwort verwenden	<p>Diese Einstellung legt fest, ob das Wi-Fi-Profil das Kennwort für die Authentifizierung enthält.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „WPA3-Enterprise“ gesetzt ist.</p>
Kennwort	<p>Diese Einstellung legt das Kennwort fest, das ein iOS-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Im Wi-Fi-Profil enthaltenes Kennwort verwenden“ ausgewählt wurde.</p>
Benutzername	<p>Diese Einstellung legt den Benutzernamen fest, den ein iOS-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „WPA3-Enterprise“ gesetzt ist.</p>
Authentifizierungstyp	<p>Diese Einstellung legt fest, welche Art der Authentifizierung ein Gerät verwendet, um eine Verbindung zum Wi-Fi-Netzwerk aufzubauen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „WPA3-Enterprise“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• Freigegebenes Zertifikat</li> <li>• SCEP</li> <li>• Benutzeranmeldeinformationen</li> </ul> <p>Der Standardwert ist „Keine“.</p>
Typ der Zertifikatverknüpfung	<p>Diese Einstellung legt den Typ der Zertifikatverknüpfung für das mit dem Wi-Fi-Profil verknüpfte Clientzertifikat fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Einzelne Referenz</li> <li>• Variable Einfügung</li> </ul> <p>Der Standardwert ist „Einzelne Referenz“.</p>

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Profil für freigegebenes Zertifikat	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.</p>
Name des Clientzertifikats	<p>Diese Einstellung legt den Namen des Clientzertifikats fest, das ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.</p>
Verknüpftes SCEP-Profil	<p>Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.</p>
Verknüpftes Profil für Benutzeranmeldeinformationen	<p>Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.</p>
<b>Vertrauen</b>	
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	<p>Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „WPA3-Enterprise“ gesetzt ist.</p>
Typ der Zertifikatverknüpfung	<p>Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „WPA3-Enterprise“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Einzelne Referenz</li> <li>• Variable Einfügung</li> </ul> <p>Der Standardwert ist „Einzelne Referenz“.</p>

<b>iOS und macOS: Wi-Fi-Profileinstellung</b>	<b>Beschreibung</b>
Profile für Zertifizierungsstellenzertifikat	<p>Diese Einstellung legt die Profile für Zertifizierungsstellenzertifikate mit den vertrauenswürdigen Zertifikaten fest, die ein Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.</p>
Vertrauenswürdige Zertifikatnamen	<p>Diese Einstellung legt die Namen der vertrauenswürdigen Zertifikate fest, die ein Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.</p>
Benutzerentscheidungen vertrauen	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „WPA3-Enterprise“ gesetzt ist.</p>
Captive-Netzwerk umgehen	<p>Diese Einstellung legt fest, ob Geräte Captive-Netzwerke umgehen können.</p>
QoS-Markierungsprofil aktivieren	<p>Diese Einstellung legt fest, ob Sie eine L2- oder L3-Markierung für Datenverkehr über das Wi-Fi-Netzwerk aktivieren können.</p>
QoS für FaceTime-Anrufe verwenden	<p>Diese Einstellung legt fest, ob Audio- und Videodatenverkehr für FaceTime-Anrufe L2- und L3-Markierungen verwenden können.</p>
Nur L2-Markierung für den QoS-Datenverkehr verwenden	<p>Diese Einstellung legt fest, ob Datenverkehr über das Wi-Fi-Netzwerk nur die L2-Markierung verwendet.</p>
QoS-Markierung auf ausgewählte Apps anwenden	<p>Diese Einstellung legt die Bundle-IDs für Apps fest, die die L2- und L3-Markierung verwenden können.</p>

## Android: Wi-Fi-Profileinstellungen

Android: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Proxy-Profil	<p>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.</p> <p>Auf Geräten mit Android 8.0 und höher, die über MDM-Steuerelemente- oder Privatsphäre des Benutzers-Aktivierungen verfügen, werden Wi-Fi-Profile mit Proxyeinstellungen nicht unterstützt. Wenn für ein Gerät mit einer dieser Aktivierungsarten ein Upgrade auf Android 8.0 durchgeführt wird, werden Wi-Fi-Profile, die mit einem Proxy-Profil verknüpft sind, vom Gerät entfernt.</p>
BSSID	<p>Diese Einstellung legt die MAC-Adresse eines drahtlosen Zugriffspunkts im Wi-Fi-Netzwerk fest.</p>
Primärer DNS	<p>Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung gilt nur für Geräte, die Samsung Knox verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.</p>
Sekundärer DNS	<p>Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung gilt nur für Geräte, die Samsung Knox verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.</p>
Sicherheitstyp	<p>Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><li>• Keine</li><li>• Persönlich</li><li>• Enterprise</li></ul> <p>Der Standardwert ist „Keine“.</p>
Persönlicher Sicherheitstyp	<p>Diese Einstellung legt den persönlichen Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Persönlich“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><li>• Keine</li><li>• WEP persönlich</li><li>• WPA-Personal/WPA2-Personal</li></ul> <p>Der Standardwert ist „Keine“.</p>



Android: Wi-Fi-Profileinstellung	Beschreibung
WEP-Schlüssel	<p>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.</p> <p>Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.</p>
Preshared key	<p>Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WPA-Personal/WPA2-Personal“ gesetzt ist.</p>
Authentifizierungsprotokoll	<p>Diese Einstellung legt die EAP-Methode fest, die das Wi-Fi-Netzwerk verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• TLS</li> <li>• TTLS</li> <li>• PEAP</li> <li>• LEAP</li> </ul> <p>Der Standardwert ist „TLS“.</p> <p>LEAP wird von Geräten, die Samsung Knox verwenden, nicht unterstützt.</p>
Interne Authentifizierung	<p>Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• PAP</li> <li>• CHAP</li> <li>• MS-CHAP</li> <li>• MS-CHAPv2</li> <li>• GTC</li> </ul> <p>Der Standardwert ist „MS-CHAPv2“.</p> <p>CHAP wird von Geräten, die Samsung Knox verwenden, nicht unterstützt.</p>

Android: Wi-Fi-Profileinstellung	Beschreibung
Externe Identität für TTLS	<p>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“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist.</p>
Externe Identität für PEAP	<p>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“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“ gesetzt ist.</p>
Benutzername	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.</p>
Im Wi-Fi-Profil enthaltenes Kennwort verwenden	<p>Diese Einstellung legt fest, ob das Wi-Fi-Profil das Kennwort für die Authentifizierung enthält.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.</p>
Kennwort	<p>Diese Einstellung legt das Kennwort fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Im Wi-Fi-Profil enthaltenes Kennwort verwenden“ ausgewählt wurde.</p>

Android: Wi-Fi-Profileinstellung	Beschreibung
Authentifizierungstyp	<p>Diese Einstellung legt fest, welche Art der Authentifizierung ein Android-Gerät verwendet, um eine Verbindung zum Wi-Fi-Netzwerk aufzubauen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• Freigegebenes Zertifikat</li> <li>• SCEP</li> <li>• Benutzeranmeldeinformationen</li> </ul> <p>Der Standardwert ist „Keine“.</p>
Typ der Zertifikatverknüpfung	<p>Diese Einstellung legt den Typ der Zertifikatverknüpfung für das mit dem Wi-Fi-Profil verknüpfte Clientzertifikat fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Einzelne Referenz</li> <li>• Variable Einfügung</li> </ul> <p>Der Standardwert ist „Einzelne Referenz“.</p>
Profil für freigegebenes Zertifikat	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.</p> <p>Der Name des Profils für das freigegebene Zertifikat muss für Geräte, die einen Knox Workspace verwenden, weniger als 36 Zeichen enthalten.</p>
Verknüpftes SCEP-Profil	<p>Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Android-Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.</p> <p>Der Name des SCEP-Profiles muss für Geräte, die einen Knox Workspace verwenden, weniger als 36 Zeichen enthalten.</p>

Android: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Profil für Benutzeranmeldeinformationen	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.</p> <p>Der Name des Profils für Benutzeranmeldeinformationen muss für Geräte, die einen Knox Workspace verwenden, weniger als 36 Zeichen enthalten.</p>
Name des Clientzertifikats	<p>Diese Einstellung legt den Namen des Clientzertifikats fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.</p>
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	<p>Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.</p>
Typ der Zertifikatverknüpfung	<p>Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Einzelne Referenz</li> <li>• Variable Einfügung</li> </ul> <p>Der Standardwert ist „Einzelne Referenz“.</p>
Zertifizierungsstellenzertifikatprofil	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.</p>
Vertrauenswürdige Zertifikatnamen	<p>Diese Einstellung legt die Namen der vertrauenswürdigen Zertifikate fest, die ein Android-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.</p>

## 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. Mögliche Werte: <ul style="list-style-type: none"><li>• Offen</li><li>• WPA-Enterprise</li><li>• WPA-Personal</li><li>• WPA2-Enterprise</li><li>• WPA2-Personal</li></ul> Der Standardwert ist „Offen“.
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. Mögliche Werte: <ul style="list-style-type: none"><li>• Keine</li><li>• WEP</li><li>• TKIP</li><li>• AES</li></ul>
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. Mögliche Werte sind 1 bis 4. Der Standardwert ist 2.

Windows: Wi-Fi-Profileinstellung	Beschreibung
Preshared key	<p>Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ gesetzt ist.</p>
Single Sign-On aktivieren	<p>Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die Authentifizierung nach einmaliger Anmeldung unterstützt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.</p>
Typ der einmaligen Anmeldung	<p>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 beim Active Directory Ihrer Organisation anmeldet. Wenn diese Einstellung auf „Direkt nach Benutzeranmeldung durchführen“ gesetzt ist, wird die einmalige Anmeldung sofort durchgeführt, nachdem sich der Benutzer beim Active Directory Ihrer Organisation angemeldet hat.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Direkt vor Benutzeranmeldung durchführen</li> <li>• Direkt nach Benutzeranmeldung durchführen</li> </ul> <p>Der Standardwert ist „Direkt vor Benutzeranmeldung durchführen“.</p>
Maximale Verzögerung für Konnektivität	<p>Diese Einstellung legt fest, wie viele Sekunden verstreichen sollen, bevor der Versuch, die Verbindung durch eine einmalige Anmeldung aufzubauen, fehlschlägt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.</p> <p>Mögliche Werte sind 0 bis 120 Sekunden.</p> <p>Der Standardwert ist 10 Sekunden.</p>
Zulassen, dass weitere Dialoge während der einmaligen Anmeldung angezeigt werden.	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.</p>

Windows: Wi-Fi-Profileinstellung	Beschreibung
Dieses Netzwerk verwendet separate virtuelle LANs für Geräte- und Benutzerauthentifizierung	<p>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 – basierend auf Berechtigungen – nach der Anmeldung des Benutzers in ein anderes VLAN-Netzwerk übergeht.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.</p>
Serverzertifikat bewerten	<p>Diese Einstellung legt fest, ob ein Gerät das Serverzertifikat bewerten muss, das die Identität des drahtlosen Zugriffspunkts überprüft.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.</p>
Benutzer nicht auffordern, neue Server oder vertrauenswürdige Zertifizierungsstellen zu autorisieren	<p>Diese Einstellung legt fest, ob ein Benutzer aufgefordert wird, dem Serverzertifikat zu vertrauen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Serverzertifikat bewerten“ ausgewählt wurde.</p>
Profile für Zertifizierungsstellenzertifil	<p>Diese Einstellung legt das Profil des Zertifizierungsstellenzertifikats fest, das den Vertrauensstamm für das vom drahtlosen Zugriffspunkt verwendete Serverzertifikat bereitstellt.</p> <p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Serverzertifikat bewerten“ ausgewählt wurde.</p>
Schnelle Wiederherstellung der Verbindung aktivieren	<p>Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die schnelle Wiederherstellung bei PEAP-Authentifizierung über mehrere drahtlose Zugriffspunkte unterstützt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.</p>
NAP erzwingen	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.</p>

Windows: Wi-Fi-Profileinstellung	Beschreibung
FIPS-Modus aktivieren	<p>Diese Einstellung gibt an, ob das Wi-Fi-Netzwerk mit dem FIPS 140-2-Standard konform ist.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA2-Enterprise“ oder „WPA2-Personal“ und der „Verschlüsselungstyp“ auf „WEP“ festgelegt sind.</p>
PMK-Zwischenspeicherung aktivieren	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA2-Enterprise“ gesetzt ist.</p>
PMK-Lebenszeit	<p>Diese Einstellung legt fest, wie viele Minuten ein Gerät den PMK im Cache speichern kann.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde.</p> <p>Mögliche Werte sind 5 bis 1440 Minuten.</p> <p>Der Standardwert ist 720 Minuten.</p>
Anzahl der Einträge im PMK-Cache	<p>Diese Einstellung legt die maximale Anzahl an PMK-Einträgen fest, die ein Gerät im Cache speichern kann.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 128.</p>
Dieses Netzwerk arbeitet mit Vorauthentifizierung	<p>Diese Einstellung legt fest, ob der Zugriffspunkt die Vorauthentifizierung für ein schnelles WPA2 Roaming unterstützt.</p> <p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde.</p>



Windows: Wi-Fi-Profileinstellung	Beschreibung
Maximale Anzahl der Vorauthentifizierungsversuche	<p>Diese Einstellung legt die maximale Anzahl zulässiger Vorauthentifizierungsversuche fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Dieses Netzwerk arbeitet mit Vorauthentifizierung“ ausgewählt wurde.</p> <p>Mögliche Werte sind 1 bis 16.</p> <p>Der Standardwert ist 3.</p>
Proxy-Typ	<p>Diese Einstellung legt den Typ der Proxy-Konfiguration für das Wi-Fi-Profil fest.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• PAC-Konfiguration</li> <li>• Manuelle Konfiguration</li> <li>• Web-Proxy automatisch erkennen</li> </ul> <p>Die Standardeinstellung ist „Manuelle Konfiguration“.</p> <p>Diese Einstellung gilt nur für Windows 10 Mobile-Geräte.</p>
PAC-URL	<p>Diese Einstellung gibt die URL für den Webserver an, der die PAC-Datei hostet, einschließlich PAC-Dateinamen im Format <code>http://&lt;web_server_URL&gt;/&lt;filename&gt;.pac</code>.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „PAC-Konfiguration“ gesetzt ist.</p>
Adresse	<p>Diese Einstellung gibt den Servernamen und Port für den Netzwerk-Proxy an. Verwenden Sie das Format „Host:Port“ (z. B. <code>server01.beispiel.com:123</code>). Der Host muss einer der folgenden sein:</p> <ul style="list-style-type: none"> <li>• Ein registrierter Name, z. B. ein Servername, FQDN oder ein einzelner Etikettenname (z. B. <code>"server01"</code> anstatt <code>server01.beispiel.com</code>)</li> <li>• Eine IPv4- oder IPv6-Adresse</li> </ul> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Manuelle Konfiguration“ gesetzt ist.</p>
Web-Proxy automatisch erkennen	<p>Diese Einstellung gibt an, ob das WPAD-Protokoll (Web Proxy Autodiscovery Protocol) für die Proxy-Suche aktiviert werden soll.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Web-Proxy automatisch erkennen“ gesetzt ist.</p> <p>Dieses Kontrollkästchen ist standardmäßig deaktiviert.</p>
Überprüfung der Internetverbindung deaktivieren	<p>Diese Einstellung legt fest, ob Überprüfungen der Internetverbindung deaktiviert werden sollen.</p> <p>Dieses Kontrollkästchen ist standardmäßig deaktiviert.</p>

Windows: Wi-Fi-Profileinstellung	Beschreibung
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.

## BlackBerry 10: Wi-Fi-Profileinstellungen

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Sicherheitstyp	<p>Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• WEP persönlich</li> <li>• WPA-Personal</li> <li>• WPA-Enterprise</li> <li>• WPA2-Personal</li> <li>• WPA2-Enterprise</li> </ul> <p>Der Standardwert ist „Keine“.</p>
WEP-Schlüssel	<p>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.</p> <p>Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abcd5“ oder „abCDefGHijKL1“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.</p>
Vorinstallierter Schlüsseltyp	<p>Diese Einstellung legt den Typ des vorinstallierten Schlüssels für das Wi-Fi-Netzwerk fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ oder „WPA2-Personal“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• ASCII</li> <li>• HEX</li> </ul> <p>Der Standardwert ist „ASCII“.</p>
Preshared key	<p>Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ oder „WPA2-Personal“ gesetzt ist.</p> <p>Mögliche Werte sind auf 64 Zeichen begrenzt.</p>

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Authentifizierungsprotokoll	<p>Diese Einstellung legt die EAP-Methode fest, die das Wi-Fi-Netzwerk verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• PEAP</li> <li>• TTLS</li> <li>• EAP-FAST</li> <li>• TLS</li> </ul> <p>Der Standardwert ist „PEAP“.</p>
Interne Authentifizierung	<p>Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit einem TLS-Tunnel verwendet wird.</p> <p>Wenn Sie PAP als interne Authentifizierungsmethode verwenden möchten, setzen Sie diese Einstellung auf „Automatisch“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“ oder „TTLS“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Automatisch</li> <li>• MS-CHAPv2</li> <li>• GTC</li> </ul> <p>Der Standardwert ist „Automatisch“.</p>
EAP-FAST-Provisionierungsmethode	<p>Diese Einstellung legt die Provisionierungsmethode für die EAP-FAST-Authentifizierung fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Anonym</li> <li>• Authentifiziert</li> </ul> <p>Der Standardwert ist „Anonym“.</p>
Benutzername	<p>Diese Einstellung legt den Benutzernamen fest, den ein BlackBerry 10-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“, „TTLS“, „EAP-FAST“ oder „TLS“ gesetzt ist.</p>

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Kennwort	<p>Diese Einstellung legt das Kennwort fest, das ein BlackBerry 10-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „PEAP“, „TTLS“ oder „EAP-FAST“ gesetzt ist.</p>
Bandtyp	<p>Diese Einstellung legt das Frequenzband fest, das vom Wi-Fi-Netzwerk verwendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Dual</li> <li>• 2,4 GHz</li> <li>• 5,0 GHz</li> </ul> <p>Der Standardwert ist „Dual“.</p>
DHCP aktivieren	<p>Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk DHCP verwendet.</p>
IP-Adresse	<p>Diese Einstellung legt die IP-Adresse des Hosts für das Wi-Fi-Netzwerk fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.</p>
Subnetzmaske	<p>Diese Einstellung legt die Subnetzmaske in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.</p>
Primärer DNS	<p>Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.</p>
Sekundärer DNS	<p>Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.</p>
Standard-Gateway	<p>Diese Einstellung legt das Standard-Gateway in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.</p>
Suffix der Domäne	<p>Diese Einstellung legt den FQDN des DNS-Suffixes fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DHCP aktivieren“ nicht ausgewählt ist.</p>
IPv6 aktivieren	<p>Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk IPv6 unterstützt.</p>

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Zugriffspunkt-Übergabe aktivieren	Diese Einstellung gibt an, ob ein BlackBerry 10-Gerät Wi-Fi-Übergaben zwischen drahtlosen Zugriffspunkten ausführen kann.
Benutzerdefinierbar	<p>Dieses Feld gibt die Wi-Fi-Funktionen an, die ein BlackBerry 10-Gerätebenutzer ändern kann. Wenn diese Einstellung auf „Schreibgeschützt“ gesetzt ist, kann der Benutzer keine Einstellung ändern. Wenn diese Einstellung auf „Nur Anmeldeinformationen“ gesetzt ist, kann der Benutzer den Benutzernamen und das Kennwort ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Schreibgeschützt</li> <li>• Nur Anmeldeinformationen</li> </ul> <p>Der Standardwert ist „Schreibgeschützt“.</p>
Datensicherheitsebene	<p>Diese Einstellung legt die Domäne im geschäftlichen Bereich fest, in der das Wi-Fi-Profil gespeichert ist, wenn der geschäftliche Bereich mit erweitertem Schutz von Daten im Ruhestand arbeitet. Diese Einstellung ist nur dann gültig, wenn die IT-Richtlinienregel „Erweiterten Schutz von Daten im Ruhestand erzwingen“ ausgewählt ist. Wenn diese Einstellung auf „Immer verfügbar“ gesetzt ist, wird das Profil in der Startdomäne gespeichert und steht zur Verfügung, wenn der geschäftliche Bereich gesperrt ist. Wenn diese Einstellung auf „Verfügbar nach Authentifizierung“ gesetzt ist, wird das Profil in der Betriebsdomäne gespeichert und ist nach dem Entsperren des geschäftlichen Bereichs so lange verfügbar, bis das Gerät erneut gestartet wird. Wenn diese Einstellung auf „Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist“ gesetzt ist, wird das Profil in der Sperrdomäne gespeichert und kann nur dann für Wi-Fi-Verbindungen verwendet werden, wenn der geschäftliche Bereich entsperrt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Immer verfügbar</li> <li>• Verfügbar nach Authentifizierung</li> <li>• Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist</li> </ul> <p>Der Standardwert ist „Immer verfügbar“.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
Erzwingen von TLS 1.2	<p>Diese Einstellung gibt an, ob die BlackBerry 10-Geräte TLS 1.2 für die Kommunikation über das Wi-Fi-Netzwerk verwenden müssen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Deaktiviert</li> <li>• Aktiviert</li> </ul> <p>Der Standardwert ist „Aus“.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
<b>Vertrauen</b>	

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Quelle des Client-Zertifikats	<p>Diese Einstellung legt fest, wie BlackBerry 10-Geräte das Client-Zertifikat abrufen können. Für den Abruf von Clientzertifikaten über die Geräte stehen vier Möglichkeiten zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Wenn Sie „SCEP“ wählen, müssen Sie auch das verknüpfte SCEP-Profil festlegen, das vom Gerät verwendet werden kann, um das Client-Zertifikat herunterzuladen.</li> <li>• Wenn Sie „Benutzeranmeldeinformationen“ wählen, müssen Sie auch das Profil für die Benutzeranmeldeinformationen festlegen, das das Gerät verwenden kann, um das Client-Zertifikat herunterzuladen.</li> <li>• Wenn Sie „Smartcard“ wählen, muss der Benutzer das Gerät mit einer Smartcard pairen, die das Client-Zertifikat enthält.</li> <li>• Wenn Sie „Sonstiges“ wählen, muss der Benutzer das Client-Zertifikat manuell zum Gerät hinzufügen.</li> </ul> <p>Smartcard-Unterstützung steht für Geräte zur Verfügung, auf denen BlackBerry 10 OS Version 10.3.1 oder höher ausgeführt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Smartcard</li> <li>• SCEP</li> <li>• Benutzeranmeldeinformationen</li> <li>• Sonstiges</li> </ul> <p>Der Standardwert ist „Sonstiges“.</p>
Verknüpftes SCEP-Profil	<p>Diese Einstellung legt das verknüpfte SCEP-Profil fest, mit dem der Benutzer eines BlackBerry 10-Geräts ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk anmeldet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „SCEP“ gesetzt ist.</p>
Verknüpftes Profil für Benutzeranmeldeinformationen	<p>Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein BlackBerry 10-Gerät verwendet, um ein Client-Zertifikat für die Authentifizierung beim Wi-Fi-Netzwerk anzumelden.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „Benutzeranmeldeinformationen“ gesetzt ist.</p> <p>Die Mindestanforderung für die Verwendung eines Profils für Benutzeranmeldeinformationen ist BlackBerry 10 OS-Version 10.3.1.</p>

BlackBerry 10: Wi-Fi-Profileinstellung	Beschreibung
Quelle des vertrauenswürdigen Zertifikats	<p>Diese Einstellung legt die Quelle des vertrauenswürdigen Zertifikats fest. Wenn diese Einstellung auf „Speicher für vertrauenswürdige Zertifikate“ gesetzt ist, kann ein BlackBerry 10-Gerät eine Verbindung zu einem Wi-Fi-Netzwerk aufbauen, das ein beliebiges Zertifikat im Wi-Fi-Zertifikatspeicher verwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• Speicher für vertrauenswürdige Zertifikate</li> </ul> <p>Der Standardwert ist „Keine“.</p>
<b>Verknüpfte Profile</b>	
Enterprise-Konnektivitäts-Profil mit BlackBerry Secure Connect Plus-Verbindung für geschäftliche Daten verwenden	<p>Diese Einstellung legt fest, ob der gesamte Datenverkehr des geschäftlichen Bereichs über BlackBerry Secure Connect Plus geleitet werden soll, selbst wenn BlackBerry 10-Geräte Zugriff auf das Wi-Fi-Netzwerk haben. Wenn Sie diese Einstellung nicht wählen, wenn Sie ein Wi-Fi-Profil konfigurieren und es BlackBerry 10-Geräten zuweisen, erhält auf den Geräten das geschäftliche Wi-Fi-Netzwerk für den Datenverkehr des geschäftlichen Bereichs Vorrang vor BlackBerry Secure Connect Plus.</p> <p>Wenn Sie diese Funktion verwenden möchten, vergewissern Sie sich, dass in der den Benutzern von BlackBerry 10-Geräten zugewiesenen IT-Richtlinie die IT-Richtlinienregel <b>Steuerung des Netzwerkzugriffs für geschäftliche Apps erzwingen</b> nicht ausgewählt ist.</p> <p>Diese Einstellung kann sich auf Datennutzung und Netzwerkkosten in Ihrem Unternehmen auswirken. Vergewissern Sie sich, dass dies die bevorzugte Konfiguration im Unternehmen ist, bevor Sie diese Funktion verwenden.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.2.</p>
Verknüpftes VPN-Profil	<p>Diese Einstellung legt das verknüpfte VPN-Profil fest, das ein BlackBerry 10-Gerät verwendet, um eine Verbindung zu einem VPN aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.</p>
Verknüpftes Proxy-Profil	<p>Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein BlackBerry 10-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.</p>

# Einrichten von geschäftlichen VPNs für Geräte

Mithilfe von VPN-Profilen können Sie festlegen, wie iOS-, macOS-, Samsung Knox-, Windows 10- und BlackBerry 10-Geräte eine Verbindung zu einem geschäftlichen VPN aufbauen. Sie können Benutzerkonten, Benutzergruppen oder Gerätegruppen ein VPN-Profil zuweisen. Bei BlackBerry 10-Geräten können Sie auch ein VPN-Profil mit einem Wi-Fi-Profil verknüpfen.

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
BlackBerry 10	Standardmäßig können sowohl geschäftliche als auch persönliche Apps die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Geschäftliche Apps können zum Herstellen einer Verbindung zum Netzwerk Ihrer Organisation auch die BlackBerry Infrastructure verwenden. Wenn die Sicherheitsrichtlinien Ihrer Organisation nicht zulassen, dass persönliche Apps auf das Netzwerk Ihrer Organisation zugreifen, können Sie die Verbindungsoptionen einschränken.
iOS	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>Sie können Per App VPN aktivieren, um das Profil nur auf die festgelegten geschäftlichen Apps anzuwenden.</p> <p>Auf dem Gerät muss eine unterstützte VPN-Client-App installiert sein. Cisco AnyConnect und Juniper werden unterstützt.</p> <p><b>Hinweis:</b> Die Juniper-App unterstützt nur SSL VPN.</p>
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.



# Erstellen eines VPN-Profiles

Die erforderlichen Profileinstellungen sind je nach Gerätetyp unterschiedlich und hängen vom VPN-Verbindungstyp und dem Authentifizierungstyp ab, die Sie ausgewählt haben.

**Hinweis:** Auf einigen Geräten kann das xAuth-Kennwort nicht gespeichert werden. Weitere Informationen [finden Sie unter support.blackberry.com/community](#) in Artikel 30353.

## 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 Benutzeranmeldeinformationen, ein SCEP-Profil oder ein Profil für ein freigegebenes Zertifikat, das Sie mit dem VPN-Profil verknüpfen.
- Erstellen Sie für iOS-, macOS-, Samsung Knox- und BlackBerry 10-Geräte, die einen Proxy-Server verwenden, ein Proxy-Profil, das mit dem VPN-Profil verknüpft werden soll. (Der Proxy-Server für Windows 10-Geräte wird im VPN-Profil konfiguriert.)
- 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. 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 VPN-Konfiguration in Ihrer Organisationsumgebung entsprechen. Wenn Ihre Organisation erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für den Zugriff auf das VPN eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername** `%UserName%` ein.
6. Wiederholen Sie Schritt 5 für jeden Gerätetyp in Ihrer Organisation.
7. Klicken Sie auf **Hinzufügen**.

## VPN-Profileinstellungen

Sie können eine Variable in einem beliebigen Textfeld der Profileinstellungen verwenden, um einen Wert zu referenzieren, statt den tatsächlichen Wert anzugeben. [VPN-Profile](#) werden auf den folgenden Gerätetypen unterstützt:

- iOS
- macOS
- Samsung Knox
- Windows 10
- BlackBerry 10

### iOS und macOS: VPN-Profileinstellungen

Bei macOS gelten Profile für Benutzerkonten oder Geräte. Sie können ein VPN-Profil konfigurieren, das entweder für Benutzerkonten oder Geräte gilt.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Profil anwenden auf	<p>Diese Einstellung gibt an, ob das VPN-Profil auf einem macOS-Gerät für das Benutzerkonto oder das Gerät gilt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Benutzer</li> <li>• Gerät</li> </ul> <p>Diese Einstellung ist nur für macOS-Geräte gültig.</p>
Verbindungstyp	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• L2TP</li> <li>• PPTP</li> <li>• IPSec</li> <li>• Cisco AnyConnect</li> <li>• Juniper</li> <li>• Pulse Secure</li> <li>• F5</li> <li>• SonicWALL Mobile Connect</li> <li>• Aruba VIA</li> <li>• Check Point Mobile</li> <li>• OpenVPN</li> <li>• Benutzerdefiniert</li> <li>• IKEv2</li> <li>• IKEv2 Immer An</li> </ul> <p>Der Standardwert ist „L2TP“.</p> <p>Einige Werte sind für macOS-Geräte nicht gültig.</p>
VPN-Bundle-ID	<p>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“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.</p>
Server	<p>Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.</p>
Benutzername	<p>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.</p>

iOS und macOS: VPN-Profileinstellung	Beschreibung
Benutzerdefinierte Schlüsselwertepaare	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.</p>
Anmeldegruppe oder Domäne	<p>Diese Einstellung legt die Anmeldegruppe oder -domäne fest, die das VPN-Gateway verwendet, um ein iOS-Gerät zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SonicWALL Mobile Connect“ gesetzt ist.</p>
Bereich	<p>Diese Einstellung legt den Namen des Authentifizierungsbereichs fest, den das VPN-Gateway verwendet, um ein iOS-Gerät zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ oder „Pulse Secure“ gesetzt ist.</p>
Rolle	<p>Diese Einstellung legt den Namen der Benutzerrolle fest, den ein VPN-Gateway verwendet, um die Netzwerkressourcen zu überprüfen, auf die ein iOS-Gerät zugreifen kann.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ oder „Pulse Secure“ gesetzt ist.</p>
Authentifizierungstyp	<p>Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest.</p> <p>Die Einstellung „Verbindungstyp“ legt fest, welche Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Kennwort</li> <li>• RSA SecurID</li> <li>• Gemeinsamer geheimer Schlüssel/Gruppenname</li> <li>• Freigegebenes Zertifikat</li> <li>• SCEP</li> <li>• Benutzeranmeldeinformationen</li> </ul>
Kennwort	<p>Diese Einstellung legt das Kennwort fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Kennwort“ gesetzt ist.</p>

iOS und macOS: VPN-Profileinstellung	Beschreibung
Gruppenname	<p>Diese Einstellung legt den Gruppennamen für das VPN-Gateway fest.</p> <p>Diese Einstellung gilt nur unter den folgenden Bedingungen:</p> <ul style="list-style-type: none"> <li>• „Anschlusstyp“ ist eingestellt auf „Cisco AnyConnect“.</li> <li>• Die Einstellung „Anschlusstyp“ ist auf „IPsec“ und die Einstellung „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt.</li> </ul>
Gemeinsamer geheimer Schlüssel	<p>Diese Einstellung legt den gemeinsamen geheimen Schlüssel für die VPN-Authentifizierung fest.</p> <p>Diese Einstellung gilt nur unter den folgenden Bedingungen:</p> <ul style="list-style-type: none"> <li>• „Anschlusstyp“ ist eingestellt auf „L2TP“.</li> <li>• Die Einstellung „Anschlusstyp“ ist auf „IPsec“ und die Einstellung „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt.</li> <li>• Die Einstellung „Anschlusstyp“ ist auf „IKEv2“ und die Einstellung „Authentifizierungsmethode“ auf „Gemeinsamer geheimer Schlüssel“ gesetzt.</li> </ul>
Profil für freigegebenes Zertifikat	<p>Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Clientzertifikat fest, das ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ oder „Authentifizierungsmethode“ auf „Freigegebenes Zertifikat“ gesetzt ist.</p>
Verknüpftes SCEP-Profil	<p>Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein iOS-Gerät verwendet, um ein Client-Zertifikat für die VPN-Authentifizierung abzurufen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ oder „Authentifizierungsmethode“ auf „SCEP“ gesetzt ist.</p>
Verknüpftes Profil für Benutzeranmeldeinformationen	<p>Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung mit dem VPN abzurufen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ oder „Authentifizierungsmethode“ auf „Benutzeranmeldeinformationen“ gesetzt ist.</p>

iOS und macOS: VPN-Profileinstellung	Beschreibung
Verschlüsselungsstufe	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „PPTP“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• Automatisch</li> <li>• Maximum</li> </ul> <p>Der Standardwert ist „Keine“.</p>
Netzwerkverkehr durch VPN leiten	<p>Diese Einstellung legt fest, ob der gesamte Netzwerkverkehr durch die VPN-Verbindung gesendet werden soll.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ oder „PPTP“ gesetzt ist.</p>
Hybrid-Authentifizierung verwenden	<p>Diese Einstellung legt fest, ob ein serverseitiges Zertifikat für die Authentifizierung verwendet wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und der „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt ist.</p>
Zur Kennworteingabe auffordern	<p>Diese Einstellung legt fest, ob ein Gerät den Benutzer zur Eingabe eines Kennworts auffordert.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“ und der „Authentifizierungstyp“ auf „Gemeinsamer geheimer Schlüssel/Gruppenname“ gesetzt ist.</p>
Zur PIN-Eingabe auffordern	<p>Diese Einstellung legt fest, ob das Gerät den Benutzer zur Eingabe einer PIN auffordert.</p> <p>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.</p>
Remote-Adresse	<p>Diese Einstellung legt die IP-Adresse bzw. den Hostnamen des VPN-Servers fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
Lokale ID	<p>Diese Einstellung legt die Identität des IKEv2-Clients in einem der folgenden Formate fest: FQDN, UserFQDN, Adresse und ASN1DN.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>

iOS und macOS: VPN-Profileinstellung	Beschreibung
Remote-ID	<p>Diese Einstellung legt die Remote-ID des IKEv2-Clients in einem der folgenden Formate fest: FQDN, Benutzer-FQDN, Adresse oder ASN1DN.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
Authentifizierungsmethode	<p>Diese Einstellung legt die Authentifizierungsmethode für das VPN fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Gemeinsamer geheimer Schlüssel</li> <li>• Freigegebenes Zertifikat</li> <li>• SCEP</li> <li>• Benutzeranmeldeinformationen</li> </ul>
VPN bei Bedarf aktivieren	<p>Diese Einstellung legt fest, ob ein Gerät automatisch beim Zugriff auf bestimmte Domänen eine VPN-Verbindung herstellen kann.</p> <p>Diese Einstellung betrifft geschäftliche Apps auf iOS-Geräten.</p> <p>Diese Einstellung gilt nur unter den folgenden Bedingungen:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Die Einstellung „Anschlusstyp“ ist auf „IKEv2“ und die „Authentifizierungsmethode“ auf „Gemeinsames Zertifikat“ gesetzt.</li> </ul>
Domänen- oder Hostnamen, die "VPN auf Abruf" verwenden können	<p>Diese Einstellung legt die Domänen und die verknüpften Aktionen für VPN bei Bedarf fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.</p> <p>Mögliche Werte für die „Bei Bedarf-Aktion“:</p> <ul style="list-style-type: none"> <li>• Immer herstellen</li> <li>• Herstellen, wenn erforderlich</li> <li>• Niemals herstellen</li> </ul>
Regeln für „VPN bei Bedarf“ für iOS 7.0 und höher	<p>Diese Einstellung legt die Verbindungsanforderungen für VPN bei Bedarf fest. Sie müssen einen oder mehrere Schlüssel aus dem Beispiel für das Nutzlastformat verwenden.</p> <p>Diese Einstellung überschreibt die Einstellung „Domänen- oder Hostnamen, die VPN bei Bedarf verwenden können“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.</p>

iOS und macOS: VPN-Profileinstellung	Beschreibung
xAuth aktivieren	<p>Diese Einstellung legt fest, ob das VPN die erweiterte Authentifizierung (xAuth) unterstützt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.</p>
TLS-Mindestversion	<p>Diese Einstellung gibt die minimale TLS Version an, die Geräte mit iOS 11 und höher für die EAP-TLS-Authentifizierung verwenden.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• 1.0</li> <li>• 1.1</li> <li>• 1.2</li> </ul> <p>Die Standardeinstellung ist „1.0“.</p>
Höchste unterstützte TLS-Version	<p>Diese Einstellung gibt die höchste unterstützte TLS Version an, die Geräte mit iOS 11 und höher für die EAP-TLS-Authentifizierung verwenden.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• 1.0</li> <li>• 1.1</li> <li>• 1.2</li> </ul> <p>Die Standardeinstellung ist „1.2“.</p>
Keep-alive-Intervall	<p>Diese Einstellung legt fest, wie häufig ein Gerät ein Keep-alive-Paket sendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Deaktiviert</li> <li>• 30 Minuten</li> <li>• 10 Minuten</li> <li>• 1 Minute</li> </ul> <p>Die Standardeinstellung ist „10 Minuten“.</p>
MOBIKE deaktivieren	<p>Diese Einstellung legt fest, ob MOBIKE deaktiviert ist.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>

iOS und macOS: VPN-Profileinstellung	Beschreibung
IKEv2-Umleitung deaktivieren	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
Perfekte Geheimhaltung bei der Weiterleitung aktivieren	<p>Diese Einstellung legt fest, ob das VPN PFS unterstützt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
NAT-Keep-alive aktivieren	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
NAT-Keep-alive-Intervall	<p>Diese Einstellung legt fest, wie häufig ein Gerät ein NAT-Keep-alive-Paket sendet (in Sekunden).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt und die Einstellung „NAT-Keep-alive aktivieren“ ausgewählt ist.</p> <p>Der Mindest- und der Standardwert ist 20.</p>
Interne IPv4- und IPv6-IKEv2-Subnetze verwenden	<p>Diese Einstellung legt fest, ob das VPN die Attribute INTERNAL_IP4_SUBNET und INTERNAL_IP6_SUBNET der IKEv2-Konfiguration verwenden kann.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
Allgemeiner Name des Serverzertifikats	<p>Diese Einstellung gibt den allgemeinen Namen in dem Zertifikat an, das der IKE-Server an das Gerät sendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
Allgemeiner Name des Serverzertifikatsausstellers	<p>Diese Einstellung gibt den allgemeinen Namen des Zertifikatsausstellers in dem Zertifikat an, das der IKE-Server an das Gerät sendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
Untergeordnete Sicherheitszuordnungsparameter anwenden	<p>Diese Einstellung gibt an, ob untergeordnete Sicherheitszuordnungsparameter angewendet werden sollen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>



iOS und macOS: VPN-Profileinstellung	Beschreibung
IKE-Sicherheitszuordnungsparameter anwenden	<p>Diese Einstellung gibt an, ob IKE-Sicherheitszuordnungsparameter angewendet werden sollen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ gesetzt ist.</p>
DH-Gruppe	<p>Diese Einstellung gibt die DH-Gruppe an, die ein Gerät zur Generierung des Schlüssels verwendet.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• 0</li> <li>• 1</li> <li>• 2</li> <li>• 5</li> <li>• 14</li> <li>• 15</li> <li>• 16</li> <li>• 17</li> <li>• 18</li> <li>• 19</li> <li>• 20</li> <li>• 21</li> <li>• 31</li> </ul> <p>Die Standardeinstellung ist „2“.</p>
Verschlüsselungsalgorithmus	<p>Diese Einstellung legt den IKE-Verschlüsselungsalgorithmus fest.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> <li>• AES 128</li> <li>• AES 256</li> <li>• AES 128 GCM</li> <li>• AES 256 GCM</li> <li>• ChaCha20Poly1305</li> </ul> <p>Die Standardeinstellung ist „3DES“.</p>

iOS und macOS: VPN-Profileinstellung	Beschreibung
Integritätsalgorithmus	<p>Diese Einstellung legt den IKE-Integritätsalgorithmus fest.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• SHA1 96</li> <li>• SHA1 160</li> <li>• SHA1 256</li> <li>• SHA2 384</li> <li>• SHA2 512</li> </ul> <p>Der Standardwert ist „SHA1-96“.</p>
Schlüsseländerungsintervall	<p>Diese Einstellung legt die Lebensdauer der IKE-Verbindung fest.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist.</p> <p>Mögliche Werte sind 10 bis 1440 Minuten.</p> <p>Der Standardwert ist 1440.</p>
Per App VPN aktivieren	<p>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.</p> <p>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“ oder „IKEv2“ gesetzt ist.</p>
Zulassen, dass Apps automatisch eine Verbindung herstellen	<p>Diese Einstellung legt fest, ob mit Per App VPN verknüpfte Apps die VPN-Verbindung automatisch starten können.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.</p>
Safari-Domänen	<p>Diese Einstellung legt die Domänen fest, die die VPN-Verbindung in Safari starten können.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.</p>

<b>iOS und macOS: VPN-Profileinstellung</b>	<b>Beschreibung</b>
Kalenderdomänen	<p>Diese Einstellung legt die Domänen fest, die die VPN-Verbindung im Kalender starten können.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.</p>
Kontaktdomänen	<p>Diese Einstellung legt die Domänen fest, die die VPN-Verbindung in Kontakten starten können.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.</p>
E-Mail-Domänen	<p>Diese Einstellung legt die Domänen fest, die die VPN-Verbindung im E-Mail-Programm starten können.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.</p>
Datenverkehrs-Tunneling	<p>Diese Einstellung legt fest, ob das VPN den Verkehr in der Anwendungsschicht oder IP-Schicht tunnelt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS 13.0 und höher.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Anwendungsschicht</li> <li>• IP-Schicht</li> </ul> <p>Die Standardeinstellung ist „Anwendungsschicht“.</p>
Verknüpftes Proxy-Profil	<p>Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein iOS-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.</p>

## Android: VPN-Profileinstellungen

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

Weitere Informationen zu den VPN-Profileinstellungen, die von Samsung Knox Workspace-Geräten unterstützt werden, finden Sie unter [Samsung Knox-VPN-JSON-Parameter](#).

<b>Android: VPN-Profileinstellung</b>	<b>Beschreibung</b>
Serveradresse	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.

Android: VPN-Profileinstellung	Beschreibung
VPN-Typ	<p>Diese Einstellung legt fest, ob ein Gerät IPsec oder SSL verwendet, um eine Verbindung mit dem Mailserver aufzubauen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• IPsec</li> <li>• SSL</li> </ul> <p>Der Standardwert ist „IPsec“.</p> <p>Die Juniper-VPN-App unterstützt nur SSL.</p>
Benutzerauthentifizierung erforderlich	<p>Diese Einstellung legt fest, ob ein Gerät einen Benutzernamen und ein Kennwort zum Herstellen einer Verbindung mit dem VPN-Server bereitstellen muss.</p>
Benutzername	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.</p>
Kennwort	<p>Diese Einstellung legt das Kennwort fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.</p>
Split-Tunnel-Typ	<p>Diese Einstellung legt fest, ob ein Gerät Split-Tunneling verwenden kann, um das VPN-Gateway zu umgehen, sofern dies vom VPN-Gateway unterstützt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Deaktiviert</li> <li>• Manuell</li> <li>• Automatisch</li> </ul> <p>Wenn der VPN-Typ auf „IPsec“ festgelegt ist, muss diese Einstellung auf „Deaktiviert“ festgelegt werden.</p> <p>Der Standardwert ist „Deaktiviert“.</p>
Weiterleitungsrouten	<p>Diese Einstellung legt die Route(n) zum Umgehen des VPN-Gateways fest. Sie können eine oder mehrere IP-Adressen angeben.</p> <p>Diese Einstellung ist nur dann gültig, wenn „VPN-Typ“ auf „SSL“ und der „Split-Tunnel-Typ“ auf „Manuell“ gesetzt ist.</p>
DPD	<p>Diese Einstellung legt fest, ob DPD aktiviert ist.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>

Android: VPN-Profileinstellung	Beschreibung
IKE-Version	<p>Diese Einstellung gibt die Version des IKE-Protokolls zur Verwendung mit der VPN-Verbindung an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• IKEv1</li> <li>• IKEv2</li> </ul> <p>Der Standardwert ist „IKEv1“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IPsec-Authentifizierungstyp	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Zertifikat</li> <li>• Preshared key</li> <li>• EAP MD5</li> <li>• EAP MSCHAPv2</li> <li>• Hybrid RSA</li> <li>• CAC-basierte Authentifizierung</li> </ul> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
ID-Typ der IPsec-Gruppe	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• IPv4-Adresse</li> <li>• Fully Qualified Domain Name (vollständiger Domänenname)</li> <li>• Benutzer-FQDN</li> <li>• IKE-Schlüssel-ID</li> </ul> <p>Wird für „IPsec-Authentifizierungstyp“ die Einstellung „Zertifikat“ verwendet, dann wird diese Einstellung automatisch auf „Standard“ festgelegt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IPsec-Gruppen-ID	<p>Diese Einstellung legt die IPsec-Gruppen-ID für die VPN-Verbindung fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>

Android: VPN-Profileinstellung	Beschreibung
Schlüsselaustauschmodus IKE-Phase-1	<p>Diese Einstellung legt den Austauschmodus für die VPN-Verbindung fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Hauptmodus</li> <li>• Aggressive-Modus</li> </ul> <p>Der Standardwert ist „Hauptmodus“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IKE-Lebensdauer	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IKE-Verschlüsselungsalgorithmus	<p>Diese Einstellung gibt den für eine IKE-Verbindung verwendeten Verschlüsselungsalgorithmus an.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IKE-Integritätsalgorithmus	<p>Diese Einstellung gibt den für eine IKE-Verbindung verwendeten Integritätsalgorithmus an.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ und die „IKE-Version“ auf „IKEv2“ gesetzt ist.</p>
IPsec DH-Gruppe	<p>Diese Einstellung gibt die DH-Gruppe an, die ein Gerät zur Generierung des Schlüssels verwendet.</p> <p>Mögliche Werte sind 0, 1, 2, 5 und 14 bis 26.</p> <p>Der Standardwert ist 0.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IPsec-Parameter	<p>Diese Einstellung legt die IPsec-Parameter für die VPN-Verbindung fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
Perfekte Geheimhaltung bei der Weiterleitung	<p>Diese Einstellung legt fest, ob das VPN-Gateway PFS unterstützt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
MOBIKE aktivieren	<p>Diese Einstellung legt fest, ob das VPN-Gateway MOBIKE unterstützt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>

Android: VPN-Profileinstellung	Beschreibung
IPsec-Lebensdauer	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IPsec-Verschlüsselungsalgorithmus	<p>Diese Einstellung legt den IPsec-Verschlüsselungsalgorithmus für die VPN-Verbindung fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.</p>
IPsec-Integritätsalgorithmus	<p>Diese Einstellung legt den IPsec-Integritätsalgorithmus für die VPN-Verbindung fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ und die „IKE-Version“ auf „IKEv2“ gesetzt ist.</p>
Authentifizierungstyp	<p>Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• Zertifikatsbasierte Authentifizierung</li> <li>• CAC-basierte Authentifizierung</li> </ul> <p>Der Standardwert ist „Keine“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.</p>
SSL-Algorithmus	<p>Diese Einstellung gibt den für eine SSL-VPN-Verbindung erforderlichen Verschlüsselungsalgorithmus an.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.</p>
UID-/PID-Informationen anhängen	<p>Diese Einstellung gibt an, ob UID/PID-Informationen an Pakete angehängt werden, die an den VPN-Client gesendet werden.</p> <p>Diese Einstellung muss für die Cisco AnyConnect VPN-App aktiviert werden.</p>
Verkettung unterstützen	<p>Diese Einstellung legt fest, wie die VPN-Verkettung unterstützt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Verkettung unterstützen</li> <li>• Äußerer Tunnel</li> <li>• Innerer Tunnel</li> </ul> <p>Der Standardwert ist „Verkettung unterstützen“.</p>

Android: VPN-Profileinstellung	Beschreibung
Typ der Anbieterzeichenfolge	<p>Diese Einstellung legt die Schlüsselwertpaare oder die JSON-Zeichenfolge für das VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Schlüsselwertpaare des Anbieters</li> <li>• JSON-Wert des Anbieters</li> </ul> <p>Der Standardwert lautet „Schlüsselwertpaare des Anbieters“.</p>
Schlüsselwertpaare des Anbieters	<p>Diese Einstellung legt die Schlüssel und die verknüpften Werte für das VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Anbieterzeichenfolge“ auf „Schlüsselwertpaare des Anbieters“ gesetzt ist.</p>
JSON-Wert des Anbieters	<p>Diese Einstellung legt die Konfigurationsdaten für die VPN-App des Anbieters im .json-Format fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Anbieterzeichenfolge“ auf „JSON-Wert des Anbieters“ gesetzt ist.</p>
Paket-ID des VPN-Clients	<p>Diese Einstellung legt die Paket-ID der VPN-App fest.</p>
Verbindung nach Fehler automatisch wiederherstellen	<p>Diese Einstellung legt fest, ob die VPN-Verbindung nach Verbindungsverlust automatisch neu hergestellt werden soll.</p>
FIPS-Modus aktivieren	<p>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.</p>
Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich	<p>Diese Einstellung gibt an, ob Samsung Knox Workspace-Geräte eine VPN-Verbindung für alle Apps im geschäftlichen Bereich oder nur für bestimmte Apps verwenden.</p> <ul style="list-style-type: none"> <li>• „Containerweites VPN“ verwendet eine VPN-Verbindung für alle Apps im geschäftlichen Bereich auf dem Gerät.</li> <li>• „Per App VPN“ verwendet nur für die angegebenen Apps eine VPN-Verbindung.</li> </ul>
Apps, die VPN-Verbindung verwenden dürfen	<p>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.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Per App VPN“ gesetzt ist.</p>
Verknüpftes Proxy-Profil	<p>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.</p>



## Windows 10: VPN-Profileinstellungen

Windows: VPN-Profileinstellung	Beschreibung
Verbindungstyp	<p>Diese Einstellung legt den Verbindungstyp fest, den ein Windows 10-Gerät für ein VPN verwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><li>• Microsoft</li><li>• Junos Pulse</li><li>• SonicWALL Mobile Connect</li><li>• F5</li><li>• Check Point Mobile</li><li>• Manuelle Verbindungsdefinition</li></ul> <p>Der Standardwert ist „Microsoft“.</p>
Server	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist.</p>
Server-URL-Liste	<p>Diese Einstellung gibt eine durch Kommas getrennte Liste von Servern mit URL, Hostname oder IP-Format an.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ nicht auf „Microsoft“ gesetzt ist.</p>
Typ der Routingrichtlinie	<p>Diese Einstellung legt den Typ der Routingrichtlinie fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><li>• Split-Tunneling</li><li>• Tunnel erzwingen</li></ul> <p>Der Standardwert ist „Tunnel erzwingen“.</p>
Nativer Protokolltyp	<p>Diese Einstellung legt den Typ der Routingrichtlinie für das VPN fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><li>• L2TP</li><li>• PPTP</li><li>• IKEv2</li><li>• Automatisch</li></ul> <p>Der Standardwert ist „Automatisch“.</p>

Windows: VPN-Profileinstellung	Beschreibung
Authentifizierung	<p>Diese Einstellung gibt die Authentifizierungsmethode für das systemeigene VPN an.</p> <p>Die Einstellung „Nativer Protokolltyp“ legt fest, welche Authentifizierungsmethoden unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird:</p> <ul style="list-style-type: none"> <li>• Wenn Sie L2TP oder PPTP auswählen, sind die möglichen Werte „MS-CHAPv2“ und „EAP“. Der Standardwert ist „MS-CHAPv2“.</li> <li>• Wenn Sie IKEv2 auswählen, sind die möglichen Werte „Benutzermethode“ und „Gerätemethode“. Der Standardwert ist „Benutzermethode“.</li> <li>• Wenn Sie „Automatisch“ auswählen, ist der einzige mögliche Wert „EAP“.</li> </ul> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• EAP</li> <li>• MS-CHAPv2</li> <li>• Benutzermethode</li> <li>• Gerätemethode</li> </ul>
EAP-Konfiguration	<p>Diese Einstellung legt die XML der EAP-Konfiguration fest.</p> <p>Weitere Informationen zum Generieren der EAP-Konfigurations-XML finden Sie unter <a href="https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration">https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration</a></p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „EAP“ gesetzt ist.</p>
Benutzermethode	<p>Diese Einstellung gibt an, dass der Typ „Benutzermethode“ zur Authentifizierung verwendet werden soll.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „Benutzermethode“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• EAP</li> </ul>
Gerätemethode	<p>Diese Einstellung gibt an, dass der Typ „Gerätemethode“ zur Authentifizierung verwendet werden soll.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „Gerätemethode“ gesetzt ist.</p> <p>Möglicher Wert:</p> <ul style="list-style-type: none"> <li>• Zertifikat</li> </ul>
Benutzerdefinierte Konfiguration	<p>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.</p> <p>Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ nicht auf „Microsoft“ gesetzt ist.</p>

<b>Windows: VPN-Profileinstellung</b>	<b>Beschreibung</b>
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.
App-Auslöserliste > App-ID	Diese Einstellung gibt eine App für ein Per App VPN an.  Mögliche Werte: <ul style="list-style-type: none"> <li>• Name der Paketfamilie. Um den Namen der Paketfamilie zu erfahren, installieren Sie die App, und führen Sie den Windows PowerShell-Befehl <code>Get-AppxPackage</code> aus. Weitere Informationen finden Sie unter <a href="http://technet.microsoft.com/en-us/library/hh856044.aspx">http://technet.microsoft.com/en-us/library/hh856044.aspx</a></li> <li>• Installationsort der App. Zum Beispiel C:\WINDOWS\System\notepad.exe.</li> </ul>
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.

<b>Windows: VPN-Profileinstellung</b>	<b>Beschreibung</b>
Filterliste für Verkehr	Diese Einstellung legt die Regeln fest, die Datenverkehr über das VPN zulassen.
Filterliste für Verkehr > App-ID	<p>Diese Einstellung gibt eine App für einen App-basierten Verkehrsfilter an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Name der Paketfamilie. Um den Namen der Paketfamilie zu erfahren, installieren Sie die App, und führen Sie den Windows PowerShell-Befehl <code>Get-AppxPackage</code> aus. Weitere Informationen finden Sie unter <a href="http://technet.microsoft.com/en-us/library/hh856044.aspx">http://technet.microsoft.com/en-us/library/hh856044.aspx</a></li> <li>• Installationsort der App. Zum Beispiel <code>C:\WINDOWS\System\notepad.exe</code>.</li> <li>• Geben Sie „SSYSTEM“ ein, um zu ermöglichen, dass der Kernel-Treiber Datenverkehr über das VPN sendet (z. B. PING oder SMB).</li> </ul>
Protokoll	<p>Diese Einstellung legt das vom VPN verwendete Protokoll fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Alle</li> <li>• TCP</li> <li>• UDP</li> </ul> <p>Der Standardwert ist „Alle“.</p>
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 Adressbereiche	Diese Einstellung gibt die Liste der zulässigen lokalen IP-Adressbereiche getrennt durch Kommas an.
Remote-Adressbereiche	Diese Einstellung gibt die Liste der zulässigen Remote-IP-Adressbereiche getrennt durch Kommas an.
Typ der Routingrichtlinie	<p>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 Verkehr über das VPN oder das Internet geleitet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Split-Tunneling</li> <li>• Tunnel erzwingen</li> </ul> <p>Die Standardeinstellung ist „Tunnel erzwingen“.</p>
Zugangsdaten speichern	Diese Einstellung gibt an, ob die Anmeldeinformationen, wann immer möglich, zwischengespeichert werden.

Windows: VPN-Profileinstellung	Beschreibung
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	<p>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:</p> <ul style="list-style-type: none"> <li>• Das Gerät bleibt mit dem VPN verbunden. Die Verbindung kann nicht getrennt werden.</li> <li>• Das Gerät muss mit diesem VPN verbunden sein, damit eine Netzwerkverbindung besteht.</li> <li>• Das Gerät kann nicht mit anderen VPN-Profilen verbunden werden oder diese ändern.</li> </ul>
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.
<b>IP-Sicherheitseigenschaften</b>	
Authentifizierungstransformationskonventionen:	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• MD596</li> <li>• SHA196</li> <li>• SHA256128</li> <li>• GCMAES128</li> <li>• GCMAE192</li> <li>• GCMAES256</li> </ul> <p>Die Standardeinstellung ist „MD596“.</p>
Chiffriertransformationskonventionen:	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• DES3</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> <li>• GCMAES128</li> <li>• GCMAES192</li> <li>• GCMAES256</li> </ul> <p>Die Standardeinstellung ist „DES“.</p>

Windows: VPN-Profileinstellung	Beschreibung
Verschlüsselungsmethode	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• DES3</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> </ul> <p>Die Standardeinstellung ist „DES“.</p>
Integritätsprüfungsmethode	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA196</li> <li>• SHA256</li> <li>• SHA384</li> </ul> <p>Die Standardeinstellung ist „MD5“.</p>
Diffie-Hellman-Gruppe	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Group1</li> <li>• Group2</li> <li>• Group14</li> <li>• ECP256</li> <li>• ECP384</li> <li>• Group24</li> </ul> <p>Die Standardeinstellung ist „Group1“.</p>
PFS-Gruppe	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• PFS1</li> <li>• PFS2</li> <li>• PFS2048</li> <li>• ECP256</li> <li>• ECP384</li> <li>• PFSMM</li> <li>• PFS24</li> </ul> <p>Der Standardwert ist „PFS1“.</p>
Proxy-Typ	<p>Diese Einstellung legt den Typ der Proxy-Konfiguration für das VPN fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• PAC-Konfiguration</li> <li>• Manuelle Konfiguration</li> </ul> <p>Der Standardwert ist „Keine“.</p>

<b>Windows: VPN-Profileinstellung</b>	<b>Beschreibung</b>
PAC-URL	<p>Diese Einstellung gibt die URL für den Webserver an, der die PAC-Datei hostet, einschließlich PAC-Dateinamen. Zum Beispiel <a href="http://www.example.com/PACfile.pac">http://www.example.com/PACfile.pac</a>.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „PAC-Konfiguration“ gesetzt ist.</p>
Adresse	<p>Diese Einstellung legt den FQDN oder die IP-Adresse eines Proxy-Servers fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Manuelle Konfiguration“ gesetzt ist.</p>
Verknüpftes SCEP-Profil	<p>Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Client-Zertifikat für die VPN-Authentifizierung abzurufen.</p>

## BlackBerry 10: VPN-Profileinstellungen

<b>BlackBerry 10: VPN-Profileinstellung</b>	<b>Beschreibung</b>
VPN bei Bedarf aktivieren	<p>Diese Einstellung legt fest, ob VPN bei Bedarf für dieses VPN-Profil aktiviert wird. Wenn diese Einstellung ausgewählt wird, legen Sie die Apps fest, die dieses VPN-Profil verwenden sollen. Nur die in diesem Profil angegebenen Apps können das Profil verwenden.</p> <p>Zur Verwendung von VPN bei Bedarf stellen Sie sicher, dass die angegebenen Apps für VPN bei Bedarf entwickelt wurden und den BlackBerry 10-Gerätebenutzern zugewiesen sind und dass dieses VPN-Profil den Gerätebenutzern zugewiesen ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS-Version 10.3.3</p>
Serveradresse	<p>Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Gateway-Typ	<p>Diese Einstellung gibt den Typ des VPN-Client an, den der VPN-Client auf einem BlackBerry 10-Gerät emuliert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Check Point VPN-1</li> <li>• Cisco VPN 3000 Series Concentrator</li> <li>• Cisco Secure PIX Firewall</li> <li>• Cisco IOS Easy VPN</li> <li>• Cisco ASA Series</li> <li>• Cisco AnyConnect</li> <li>• Juniper SRX Series (IPsec VPN)</li> <li>• Juniper MAG Series oder Juniper SA Series (SSL VPN)</li> <li>• Microsoft IKEv2 VPN-Server</li> <li>• Generischer IKEv2 VPN-Server</li> <li>• Mit NIAP kompatibler IKEv2 VPN-Server</li> </ul> <p>Der Standardwert ist „Check Point VPN-1“.</p>
Authentifizierungstyp	<p>Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest.</p> <p>Die Einstellung „Gatewaytyp“ legt fest, welche Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• PSK</li> <li>• PKI</li> <li>• XAUTH-PSK</li> <li>• XAUTH-PKI</li> <li>• EAP-TLS</li> <li>• EAP-MS-CHAPv2</li> </ul>
Vorinstallierter Schlüssel oder Gruppenkennwort	<p>Diese Einstellung legt den vorinstallierten Schlüssel oder das Gruppenkennwort für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „PSK“ oder „XAUTH-PSK“ gesetzt ist.</p>
Benutzername	<p>Diese Einstellung legt den Benutzernamen fest, den ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ oder die Einstellung „Authentifizierungstyp“ auf „XAUTH-PSK“ oder „XAUTH-PKI“ gesetzt ist.</p>
Hardware-Token	<p>Diese Einstellung legt fest, ob ein Benutzer ein Hardware-Token verwenden muss, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „XAUTH-PSK“ oder „XAUTH-PKI“ gesetzt ist.</p>



BlackBerry 10: VPN-Profileinstellung	Beschreibung
Kennwort	<p>Diese Einstellung legt das Kennwort fest, den ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ oder die Einstellung „Authentifizierungstyp“ auf „XAUTH-PSK“ oder „XAUTH-PKI“ gesetzt und die Einstellung „Hardware-Token“ nicht ausgewählt ist.</p>
EAP-Identität	<p>Diese Einstellung legt die EAP-Identität fest, die ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-TLS“ gesetzt ist.</p>
EAP-TLS Gateway-ID	<p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ und der „Authentifizierungstyp“ auf „EAP-TLS“ festgelegt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
MS-CHAPv2 EAP-Identität	<p>Diese Einstellung legt die MS-CHAPv2 EAP-Identität fest, die ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-MS-CHAPv2“ gesetzt ist.</p>
MS-CHAPv2-Benutzername	<p>Diese Einstellung legt den MS-CHAPv2-Benutzernamen fest, den ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-MS-CHAPv2“ gesetzt ist.</p>
MS-CHAPv2-Kennwort	<p>Diese Einstellung legt das MS-CHAPv2-Kennwort fest, das ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „EAP-MS-CHAPv2“ gesetzt ist.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Authentifizierungs-ID-Typ	<p>Diese Einstellung legt den Authentifizierungs-ID-Typ für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Einstellung „Gatewaytyp“ legt fest, welche Authentifizierungs-ID-Typen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• IPv4</li> <li>• Fully Qualified Domain Name (vollständiger Domänenname)</li> <li>• E-Mail-Adresse</li> <li>• Identitätszertifikat – Distinguished Name</li> <li>• Identitätszertifikat – Allgemeiner Name</li> <li>• Schlüssel-ID</li> </ul>
Authentifizierungs-ID oder Gruppenbenutzername	<p>Diese Einstellung legt die Authentifizierungs-ID oder den Gruppenbenutzernamen für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist oder wenn die Einstellung „Authentifizierungstyp“ auf „PSK“ oder „XAUTH-PSK“ gesetzt ist.</p>
Gateway-Authentifizierungstyp	<p>Diese Einstellung legt den Gateway-Authentifizierungstyp für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• PSK</li> <li>• PKI</li> </ul> <p>Der Standardwert ist „Keine“.</p>
OCSP- und CRL-Prüfungen für Zertifikate aus dem VPN aktivieren	<p>Diese Einstellung ermöglicht die Zertifikatwiderrufsprüfung für die bei der Authentifizierung verwendeten Zertifikate.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ und die Einstellung „Authentifizierungstyp“ auf „PKI“ oder „EAP-TLS“ festgelegt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Vorinstallierter Gateway-Schlüssel	<p>Diese Einstellung legt den vorinstallierten Gateway-Schlüssel für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gateway-Authentifizierungstyp“ auf „PSK“ gesetzt ist.</p>
Gateway-Authentifizierungs-ID-Typ	<p>Diese Einstellung legt den Gateway-Authentifizierungs-ID-Typ für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Juniper MAG Series oder Juniper SA Series (SSL VPN)“, „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• IPv4</li> <li>• Fully Qualified Domain Name (vollständiger Domänenname)</li> <li>• E-Mail-Adresse</li> <li>• Identitätszertifikat – Distinguished Name</li> <li>• Identitätszertifikat – Allgemeiner Name</li> <li>• Schlüssel-ID</li> </ul> <p>Der Standardwert ist „IPv4“.</p>
Gateway-Authentifizierungs-ID	<p>Diese Einstellung legt die Gateway-Authentifizierungs-ID für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gateway-Authentifizierungs-ID“ auf „Vollständig qualifizierter Domänenname“ oder „E-Mail-Adresse“ gesetzt ist.</p>
Senden einer weiteren Gateway-Request-ID in Nachricht 1 des IKEv2-Protokolls	<p>Der Standardwert ist „Deaktiviert“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS-Version 10.3.3</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Angeforderter Gateway-ID-Typ	<p>Diese Einstellung gibt den Typ der angeforderten Gateway-ID für das VPN an.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP-kompatibler IKEv2 VPN-Server“ festgelegt ist und die Einstellung „Senden der erforderlichen Gateway-ID in Nachricht 1 des IKEv2-Protokolls“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• IPv4</li> <li>• Fully Qualified Domain Name (vollständiger Domänenname)</li> <li>• E-Mail-Adresse</li> <li>• Identitätszertifikat – Distinguished Name</li> <li>• Identitätszertifikat – Allgemeiner Name</li> <li>• Schlüssel-ID</li> </ul> <p>Der Standardwert ist „IPv4“.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS-Version 10.3.3</p>
Angeforderte Gateway-ID	<p>Diese Einstellung fordert bei der Anmeldung eine bestimmte Gateway-ID in der ersten IKE-Nachricht an, wenn der VPN-Server mehrere IDs unterstützt. Diese kann sich von der Gateway-ID für die Authentifizierung unterscheiden.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP-kompatibler IKEv2 VPN-Server“ festgelegt ist und die Einstellung „Senden der erforderlichen Gateway-ID in Nachricht 1 des IKEv2-Protokolls“ ausgewählt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Sekundärer Benutzername	<p>Diese Einstellung legt den Benutzernamen fest, den ein BlackBerry 10-Gerät für die Sekundär-Authentifizierung beim VPN-Gateway verwendet. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
Sekundäres Kennwort	<p>Diese Einstellung legt das Kennwort fest, das ein BlackBerry 10-Gerät für die Sekundär-Authentifizierung mit dem VPN-Gateway verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
Gruppenname	<p>Diese Einstellung legt den Gruppennamen für das VPN-Gateway fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Automatische Clientzertifikatsverarbeitung aktivieren	<p>Diese Einstellung legt fest, ob ein Clientzertifikat automatisch ausgewählt wird, wenn eine VPN-Verbindung hergestellt wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
IPsec-Authentifizierung aktivieren	<p>Diese Einstellung legt fest, ob das VPN-Gateway die IPsec-Authentifizierung verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
IPsec-Authentifizierungstyp	<p>Diese Einstellung legt den Authentifizierungstyp für eine IPsec VPN-Verbindung fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „IPsec-Authentifizierung aktivieren“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• EAP-MS-CHAPv2</li> <li>• EAP-MD5</li> <li>• EAP-GTC</li> <li>• EAP-AnyConnect</li> <li>• IKE-RSA</li> </ul> <p>Der Standardwert ist EAP-MS-CHAPv2.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
EAP-Authentifizierungs-ID	<p>Diese Einstellung legt die EAP-Identität fest, die ein BlackBerry 10-Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „IPsec-Authentifizierungstyp“ auf „EAP MSCHAPv2“, „EAP MD5“ oder „EAP GTC“ gesetzt ist.</p>
Subnetze ausschließen	<p>Diese Einstellung legt fest, ob bestimmte Subnetze von der Verwendung der VPN-Verbindung ausgenommen werden.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
Ausgeschlossene Subnetze	<p>Diese Einstellung legt die Subnetze und die Subnetzmasken fest, die nicht über die VPN-Verbindung gesendet werden.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Subnetzmarkierung deaktivieren“ ausgewählt ist.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Cisco AnyConnect-Konfigurationsdatei (.xml)	<p>Diese Einstellung legt den Speicherort der Cisco AnyConnect-Konfigurationsdatei fest, die an BlackBerry 10-Geräte gesendet wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Cisco AnyConnect“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
Persönliche Apps in geschäftlichen Netzwerken zulassen	<p>Diese Einstellung legt fest, ob persönliche Apps auf einem BlackBerry 10-Gerät eine VPN-Verbindung verwenden können.</p> <p>Diese Einstellung ist nur dann gültig, wenn die IT-Richtlinienregel „Zulassen, dass persönliche Apps geschäftliche Netzwerke verwenden“ ausgewählt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
Aktion bei nicht vertrauenswürdigem Zertifikat	<p>Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät nicht vertrauenswürdige Zertifikate annimmt. Wenn die Einstellung auf „Zulassen“ gesetzt ist, nimmt das Gerät nicht vertrauenswürdige Zertifikate automatisch an. Wenn die Einstellung auf „Eingabeaufforderung“ gesetzt ist, kann der Benutzer entscheiden, ob er nicht vertrauenswürdige Zertifikate annehmen möchte. Wenn diese Einstellung auf „Nicht zulassen“ gesetzt ist, lehnt das Gerät nicht vertrauenswürdige Zertifikate ab.</p> <p>Die Einstellung „Gatewaytyp“ legt fest, welche nicht vertrauenswürdigen Zertifikataktionen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• zulassen</li> <li>• Eingabeaufforderung</li> <li>• Nicht zulassen</li> </ul> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.2.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Quelle des Client-Zertifikats	<p>Diese Einstellung legt fest, wie BlackBerry 10-Geräte das Client-Zertifikat abrufen können. Für den Abruf von Clientzertifikaten über die Geräte stehen vier Möglichkeiten zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Wenn Sie „Smartcard“ wählen, muss der Benutzer das Gerät mit einer Smartcard koppeln, die das Clientzertifikat enthält.</li> <li>• Wenn Sie „SCEP“ wählen, müssen Sie auch das verknüpfte SCEP-Profil festlegen, das vom Gerät verwendet werden kann, um das Clientzertifikat herunterzuladen.</li> <li>• Wenn Sie „Benutzeranmeldeinformationen“ wählen, müssen Sie auch das Profil für Benutzeranmeldeinformationen festlegen, das das Gerät verwenden kann, um das Clientzertifikat herunterzuladen.</li> <li>• Wenn Sie „Sonstiges“ wählen, muss der Benutzer das Clientzertifikat manuell zum Gerät hinzufügen.</li> </ul> <p>Smartcard-Unterstützung steht für Geräte zur Verfügung, auf denen BlackBerry 10 OS Version 10.3.1 oder höher ausgeführt wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „PKI“ oder „XAUTH-PKI“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Smartcard</li> <li>• SCEP</li> <li>• Benutzeranmeldeinformationen</li> <li>• Sonstiges</li> </ul> <p>Der Standardwert ist „Sonstiges“.</p>
Verknüpftes SCEP-Profil	<p>Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein BlackBerry 10-Gerät verwendet, um ein Clientzertifikat für die VPN-Authentifizierung abzurufen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „SCEP“ gesetzt ist.</p>
Verknüpftes Profil für Benutzeranmeldeinformationen	<p>Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein BlackBerry 10-Gerät verwendet, um ein Clientzertifikat für die Authentifizierung mit dem VPN abzurufen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Quelle des Client-Zertifikats“ auf „Benutzeranmeldeinformationen“ gesetzt ist.</p> <p>Die Mindestanforderung für die Verwendung eines Profils für Benutzeranmeldeinformationen ist BlackBerry 10 OS Version 10.3.1.</p>
IKE-Lebensdauer	<p>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 BlackBerry 10-Geräts verwendet.</p> <p>Mögliche Werte sind 1 bis 2.147.483.647.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
IKE-Schwellenwert	<p>Mit dieser Einstellung legen Sie den Prozentsatz der IKE-Lebensdauer fest, bei dem der VPN-Client den Austausch eines neuen Schlüssels initiiert.</p> <p>Mögliche Werte: 0-100 %</p> <p>Der Standardwert ist „90“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
IPsec-Lebensdauer	<p>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 BlackBerry 10-Geräts verwendet.</p> <p>Mögliche Werte sind 1 bis 2.147.483.647.</p>
Schwellenwert für IPSec	<p>Mit dieser Einstellung legen Sie den Prozentsatz des Schwellenwerts für IPSec fest, bei dem der VPN-Client den Austausch eines neuen Schlüssels initiiert.</p> <p>Mögliche Werte: 0-100 %</p> <p>Der Standardwert ist „90“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
VPN-Erweiterungen zulassen	<p>Mit dieser Einstellung können Sie Erweiterungen aktivieren oder deaktivieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Liste der VPN-Erweiterungen	<p>Mit dieser Einstellung können Sie eine Liste der Erweiterungen erstellen, die verwendet werden, um Anbieter-ID-Payloads zu generieren und zusätzliche Zertifikatsüberprüfungen auszuführen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ festgelegt ist und die Einstellung „VPN-Erweiterungen zulassen“ ausgewählt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Erweiterung für Anbieter-ID erforderlich	<p>Diese Einstellung gibt an, dass der Administrator eine der Erweiterungen aus der Liste der VPN-Erweiterungen verwenden möchte, um während der Anmeldung ein Anbieter-ID-Payload zu generieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ festgelegt ist und die Einstellung „VPN-Erweiterungen zulassen“ ausgewählt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>



BlackBerry 10: VPN-Profileinstellung	Beschreibung
Erweiterung für Zertifikatsüberprüfung erforderlich	<p>Diese Einstellung gibt an, dass der Administrator eine der Erweiterungen verwenden möchte, um eine zusätzliche Zertifikatsüberprüfung durchzuführen.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ festgelegt ist und die Einstellung „VPN-Erweiterungen zulassen“ ausgewählt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Sitzungswiederaufnahme aktivieren	<p>Diese Einstellung aktiviert die Einstellungen der IKEv2-Sitzungswiederaufnahme. Wenn der VPN-Server diese Funktion unterstützt, wird der VPN-Client die Sitzung unterbrechen und fortsetzen, anstatt sie komplett zu trennen und die Verbindung erneut aufzubauen, sobald die automatische VPN-Verbindung aktiviert wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Ticket-Schwellenwert	<p>Mit dieser Einstellung legen Sie fest, bei welchem Prozentsatz des Ticket-Schwellenwerts eine Sitzungswiederaufnahme stattfinden wird.</p> <p>Mögliche Werte: 0-100 %</p> <p>Der Standardwert ist „90“.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ festgelegt und die Einstellung „Sitzungswiederaufnahme aktivieren“ ausgewählt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Zertifikatnutzlasten im Hash-und-URL-Format während IKE aktivieren	<p>Diese Einstellung gibt an, ob der VPN-Client dem VPN-Server anzeigt, dass er die Verwendung von IKEv2 zum Austausch von Zertifikaten mithilfe von URLs unterstützt, und dass er ggf. Zertifikate von einer angegebenen HTTP-URL abruft.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Strikte Anwendung der zugelassenen Algorithmen aktivieren	<p>Diese Einstellung gibt an, ob die Verwendung der von NIAP zugelassenen Algorithmen strikt durchgesetzt wird.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.3.</p>
Split-Tunneling	<p>Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät Split-Tunneling verwenden kann, um das VPN-Gateway zu umgehen, sofern vom VPN-Gateway unterstützt.</p> <p>Diese Einstellung ist nicht gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Banner deaktivieren	<p>Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät das VPN-Banner blockiert.</p> <p>Diese Einstellung ist nicht gültig, wenn die Einstellung „Gatewaytyp“ auf „Mit NIAP kompatibler IKEv2 VPN-Server“ gesetzt ist.</p>
Quelle des vertrauenswürdigen Zertifikats	<p>Diese Einstellung legt die Quelle des vertrauenswürdigen Zertifikats fest. Wenn diese Einstellung auf „Speicher für vertrauenswürdige Zertifikate“ gesetzt ist, kann ein BlackBerry 10-Gerät eine Verbindung zu einem VPN aufbauen, das ein beliebiges Zertifikat im VPN-Zertifikatspeicher verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „PKI“ oder „XAUTH-PKI“ gesetzt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• Speicher für vertrauenswürdige Zertifikate</li> </ul> <p>Der Standardwert ist „Keine“.</p>
IP automatisch ermitteln	<p>Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die IP-Konfiguration des VPN-Gateways automatisch ermittelt.</p>
Private IP	<p>Diese Einstellung legt die private IP des VPN-Gateways fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.</p>
Private IP-Maske	<p>Diese Einstellung legt die private IP-Maske des VPN-Gateways fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.</p>
Subnetz	<p>Diese Einstellung legt das Subnetz des VPN-Gateways fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.</p>
Subnetzmaske	<p>Diese Einstellung legt die Subnetzmaske des VPN-Gateways fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „IP automatisch ermitteln“ nicht ausgewählt ist.</p>
DNS automatisch ermitteln	<p>Diese Einstellung legt fest, ob ein BlackBerry 10-Gerät die DNS-Konfiguration des VPN-Gateways automatisch ermittelt.</p>
Primärer DNS	<p>Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DNS automatisch ermitteln“ nicht ausgewählt ist.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Sekundärer DNS	<p>Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“).</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DNS automatisch ermitteln“ nicht ausgewählt ist.</p>
Suffix der Domäne	<p>Diese Einstellung legt den FQDN des DNS-Suffixes fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „DNS automatisch ermitteln“ nicht ausgewählt ist.</p>
Perfekte Geheimhaltung bei der Weiterleitung	<p>Diese Einstellung legt fest, ob das VPN-Gateway PFS unterstützt.</p> <p>Wenn diese Einstellung ausgewählt ist, darf die Einstellung „IKE IPSec DH-Gruppe“ nicht auf „0“ gesetzt werden.</p>
Manuelle Algorithmenauswahl	<p>Diese Einstellung legt fest, ob Sie die kryptografischen Algorithmen für das VPN-Gateway einrichten müssen.</p>
IKE DH-Gruppe	<p>Diese Einstellung gibt die DH-Gruppe an, die ein BlackBerry 10-Gerät zur Generierung des Schlüssels verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• 1 bis 26 außer 3, 4 und 6</li> <li>• Benutzerdefiniert 1 bis Benutzerdefiniert 5</li> </ul> <p>Der Standardwert ist „1“.</p>
Provider für benutzerdefinierte IKE DH	<p>Diese Einstellung legt den Namen des Providers für die benutzerdefinierte IKE DH fest.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „IKE DH-Gruppe“ auf einen der benutzerdefinierten Werte gesetzt ist.</p>
MOBIKE aktivieren	<p>Diese Einstellung legt fest, ob das VPN-Gateway MOBIKE unterstützt.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Gatewaytyp“ auf „Microsoft IKEv2 VPN-Server“ oder „Generischer IKEv2 VPN-Server“ gesetzt ist oder wenn die Einstellung „Authentifizierungstyp“ auf „PKI“ und die Einstellung für die „IKE DH-Gruppe“ auf einen der benutzerdefinierten Werte gesetzt ist.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
IKE: Chiffrierschlüssel	<p>Diese Einstellung legt den Algorithmus fest, den ein BlackBerry 10-Gerät verwendet, um einen gemeinsam verwendeten geheimen Schlüssel zu generieren.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• DES (56-Bit-Schlüssel)</li> <li>• Triple DES (168-Bit-Schlüssel)</li> <li>• AES (128-Bit-Schlüssel)</li> <li>• AES (192-Bit-Schlüssel)</li> <li>• AES (256-Bit-Schlüssel)</li> </ul> <p>Der Standardwert ist „Keine“.</p>
IKE-Hash	<p>Diese Einstellung legt die Hash-Funktion fest, die ein BlackBerry 10-Gerät mit IKE verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• MD5</li> <li>• AES-XCBC</li> <li>• SHA-1</li> <li>• SHA-256</li> <li>• SHA-384</li> <li>• SHA-512</li> </ul> <p>Der Standardwert ist „Keine“.</p>
IKE PRF	<p>Diese Einstellung legt die PRF-Funktion fest, die ein BlackBerry 10-Gerät mit IKE verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• HMAC</li> <li>• HMAC-MD5</li> <li>• AES-XCBC</li> <li>• HMAC-SHA-1</li> <li>• HMAC-SHA-256</li> <li>• HMAC-SHA-384</li> <li>• HMAC-SHA-512</li> </ul> <p>Der Standardwert ist „Keine“.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
IPsec DH-Gruppe	<p>Diese Einstellung legt die DH-Gruppe fest, die ein BlackBerry 10-Gerät mit IPsec verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.</p> <p>Mögliche Werte sind 0 bis 26 außer 3, 4 und 6.</p> <p>Der Standardwert ist „0“.</p>
IPsec: Chiffrierschlüssel	<p>Diese Einstellung legt den Algorithmus fest, den ein BlackBerry 10-Gerät mit IPsec verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• DES (56-Bit-Schlüssel)</li> <li>• Triple DES (168-Bit-Schlüssel)</li> <li>• AES (128-Bit-Schlüssel)</li> <li>• AES (192-Bit-Schlüssel)</li> <li>• AES (256-Bit-Schlüssel)</li> </ul> <p>Der Standardwert ist „Keine“.</p>
IPsec-Hash	<p>Diese Einstellung legt die Hash-Funktion fest, die ein BlackBerry 10-Gerät mit IPsec verwendet.</p> <p>Diese Einstellung ist nur dann gültig, wenn die Einstellung „Manuelle Algorithmenauswahl“ ausgewählt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Keine</li> <li>• MD5</li> <li>• AES-XCBC</li> <li>• SHA-1</li> <li>• SHA-256</li> <li>• SHA-384</li> <li>• SHA-512</li> </ul> <p>Der Standardwert ist „Keine“.</p>
NAT-Keep-alive	<p>Diese Einstellung legt fest, wie häufig ein Gerät ein NAT-Keep-alive-Paket sendet. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des BlackBerry 10-Geräts verwendet.</p> <p>Mögliche Werte sind 1 bis 2.147.483.647.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
DPD-Frequenz	<p>Diese Einstellung legt die DPD-Frequenz in Sekunden fest. Ein BlackBerry 10-Gerät unterstützt eine Mindesteinstellung von 10 Sekunden. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet.</p> <p>Mögliche Werte sind 1 bis 2.147.483.647.</p>
Benutzerdefinierbar	<p>Dieses Feld gibt die VPN-Funktionen an, die ein BlackBerry 10-Gerätebenutzer ändern kann. Wenn diese Einstellung auf „Schreibgeschützt“ gesetzt ist, kann der Benutzer keine Einstellung ändern. Wenn diese Einstellung auf „Nur Anmeldeinformationen“ gesetzt ist, kann der Benutzer den Benutzernamen und das Kennwort ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Schreibgeschützt</li> <li>• Nur Anmeldeinformationen</li> </ul> <p>Der Standardwert ist „Schreibgeschützt“.</p>
VPN-Informationen auf Gerät anzeigen	<p>Diese Einstellung legt fest, ob VPN-Informationen auf einem BlackBerry 10-Gerät angezeigt werden. Wenn diese Einstellung auf „Sichtbar“ gesetzt ist, werden die meisten Informationen des VPN-Profiles auf dem Gerät angezeigt. Wenn diese Einstellung auf „Unsichtbar“ gesetzt ist, wird nur der Profilname auf dem Gerät angezeigt. Wenn diese Einstellung auf „Nur Anmeldeinformationen“ gesetzt ist, werden nur die Felder für den Profilnamen und die Anmeldeinformationen auf dem Gerät angezeigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Sichtbar</li> <li>• Unsichtbar</li> <li>• Nur Anmeldeinformationen</li> </ul> <p>Der Standardwert ist „Sichtbar“.</p>

BlackBerry 10: VPN-Profileinstellung	Beschreibung
Datensicherheitsebene	<p>Diese Einstellung legt die Domäne im geschäftlichen Bereich fest, in der das VPN-Profil gespeichert ist, wenn der geschäftliche Bereich mit erweitertem Schutz von Daten im Ruhestand arbeitet. Diese Einstellung ist nur dann gültig, wenn die IT-Richtlinienregel „Erweiterten Schutz von Daten im Ruhestand erzwingen“ ausgewählt ist. Wenn diese Einstellung auf „Immer verfügbar“ gesetzt ist, wird das Profil in der Startdomäne gespeichert und steht zur Verfügung, wenn der geschäftliche Bereich gesperrt ist. Wenn diese Einstellung auf „Verfügbar nach Authentifizierung“ gesetzt ist, wird das Profil in der Betriebsdomäne gespeichert und ist nach dem Entsperren des geschäftlichen Bereichs so lange verfügbar, bis das Gerät erneut gestartet wird. Wenn diese Einstellung auf „Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist“ gesetzt ist, wird das Profil in der Sperrdomäne gespeichert und kann nur dann für VPN-Verbindungen verwendet werden, wenn der geschäftliche Bereich entsperrt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Immer verfügbar</li> <li>• Verfügbar nach Authentifizierung</li> <li>• Nur verfügbar, wenn der geschäftliche Bereich entsperrt ist</li> </ul> <p>Der Standardwert ist „Immer verfügbar“.</p> <p>Die Mindestanforderung ist BlackBerry 10 OS, Version 10.3.1.</p>
Verknüpftes Proxy-Profil	<p>Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein BlackBerry 10-Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.</p>

## Per App VPN aktivieren

Sie können Per App VPN auf iOS-, Samsung Knox- und Windows 10-Geräten einrichten, um zu bestimmen, welche Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Ein Per-App-VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (z. B. 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.

Für iOS-Geräte sind Apps mit einem VPN-Profil verknüpft, wenn Sie die App oder App-Gruppe einem Benutzer, einer Benutzergruppe oder einer Gerätegruppe zuweisen.

Für Samsung Knox-Geräte mit Android Enterprise- und Samsung Knox Workspace-Aktivierung werden im VPN-Profil Apps der Einstellung „Apps, die VPN-Verbindung verwenden dürfen“ hinzugefügt.

Für Windows 10-Geräte werden im VPN-Profil Apps der Einstellung „App-Auslöserliste“ hinzugefügt.

### So wählt BlackBerry UEM die Per App VPN-Einstellungen für die Zuweisung zu iOS-Geräten aus

Einer App oder einer App-Gruppe kann nur ein VPN-Profil zugewiesen werden. BlackBerry UEM verwendet die folgenden Regeln, um zu bestimmen, welche Per App VPN-Einstellungen einer App auf iOS-Geräten zugewiesen werden:

- Per App VPN-Einstellungen, die direkt mit einer App verknüpft sind, haben Vorrang vor Per App VPN-Einstellungen, die indirekt durch eine App-Gruppe verknüpft sind.
- Per App VPN-Einstellungen, die direkt mit einem Benutzer verknüpft sind, haben Vorrang vor Per App VPN-Einstellungen, die indirekt durch eine Benutzergruppe verknüpft sind.
- Per App VPN-Einstellungen, die mit einer benötigten App verknüpft sind, haben Vorrang vor Per App VPN-Einstellungen, die einer optionalen Instanz der gleichen App zugewiesen sind.
- Per App VPN-Einstellungen, die mit dem Benutzergruppennamen verknüpft sind, der weiter oben in der alphabetischen Liste angezeigt wird, haben Vorrang, wenn 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-, macOS-, Android- und BlackBerry 10-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
BlackBerry 10	<p>Erstellen Sie ein Proxy-Profil, und ordnen Sie es den von Ihrer Organisation verwendeten Profilen zu, zu denen folgende gehören können:</p> <ul style="list-style-type: none"><li>• Wi-Fi</li><li>• VPN</li><li>• Enterprise-Konnektivität</li></ul>
iOS	<p>Erstellen Sie ein Proxy-Profil, und ordnen Sie es den von Ihrer Organisation verwendeten Profilen zu, zu denen folgende gehören können:</p> <ul style="list-style-type: none"><li>• Wi-Fi</li><li>• VPN</li></ul> <p>Sie können auch den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Proxy-Profil zuweisen.</p> <p><b>Hinweis:</b> 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.</p>
macOS	<p>Erstellen Sie ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi- oder VPN-Profil.</p> <p>Bei macOS gelten Profile für Benutzerkonten oder Geräte. Proxy-Profile gelten für Geräte.</p>
Android	<p>Erstellen Sie für Android Enterprise-Geräte ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi-Profil.</p> <p>Auf Geräten mit Android 8.0 und höher, die über MDM-Steuerelemente- oder Privatsphäre des Benutzers-Aktivierungen verfügen, werden Wi-Fi-Profile mit Proxyeinstellungen nicht unterstützt. Wenn für ein Gerät mit einer dieser Aktivierungsarten ein Upgrade auf Android 8.0 durchgeführt wird, werden Wi-Fi-Profile, die mit einem Proxy-Profil verknüpft sind, vom Gerät entfernt.</p>

Gerät	Proxy-Konfiguration
Samsung Knox	<p>Erstellen Sie ein Proxy-Profil, und verknüpfen Sie es mit den Profilen, die Ihr Unternehmen nutzt. Es gelten folgende Bedingungen:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p><b>Hinweis:</b> Für die Verwendung eines Proxy-Profiles mit einem Enterprise-Konnektivitätsprofil muss BlackBerry Secure Connect Plus aktiviert sein.</p> <p>Sie können auch den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Proxy-Profil zuweisen. Es gelten folgende Bedingungen:</p> <ul style="list-style-type: none"> <li>• Auf Knox Workspace-Geräten und Samsung Knox-Geräten mit Android Enterprise-Aktivierungen bestimmt das Profil die Browser-Proxy-Einstellungen des geschäftlichen Bereichs.</li> <li>• Auf Samsung Knox-MDM-Geräten bestimmt das Profil die Browser-Proxy-Einstellungen des Geräts.</li> </ul> <p><b>Hinweis:</b> PAC-Konfiguration wird auf Knox Workspace-Geräten mit Knox 2.5 und früher und Knox-MDM-Geräten nicht unterstützt.</p>
Windows 10	<p>Erstellen Sie ein Wi-Fi- oder VPN-Profil, und geben Sie die Proxy-Serverinformationen in den Profileinstellungen an. Es gelten folgende Bedingungen:</p> <ul style="list-style-type: none"> <li>• Wi-Fi-Proxy unterstützt nur manuelle Konfiguration und ist nur mit Windows 10 Mobile-Geräten kompatibel.</li> <li>• VPN-Proxy unterstützt PAC oder manuelle Konfiguration.</li> </ul>

## Erstellen eines Proxy-Profiles

Wenn Ihre Organisation eine PAC-Datei zur Definition von Proxy-Regeln verwendet, können Sie die PAC-Konfiguration auswählen, um die Einstellungen des Proxy-Servers aus der von Ihnen festgelegten PAC-Datei zu verwenden. Andernfalls können Sie die manuelle Konfiguration auswählen und die Einstellungen des Proxy-Servers direkt im Profil festlegen.

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	<ol style="list-style-type: none"> <li>a. Vergewissern Sie sich, dass in der Dropdown-Liste <b>Typ</b> die Option <b>PAC-Konfiguration</b> ausgewählt ist.</li> <li>b. Geben Sie im Feld <b>PAC-URL</b> die URL für den Webserver an, der die PAC-Datei hostet, sowie den PAC-Dateinamen (zum Beispiel <code>http://www.example.com/PACfile.pac</code>). Die PAC-Datei sollte nicht auf einem Server gehostet werden, der BlackBerry UEM oder eine seiner Komponenten hostet.</li> <li>c. Führen Sie auf der Registerkarte <b>BlackBerry</b> die folgenden Aktionen aus: <ol style="list-style-type: none"> <li>1. 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 <b>Benutzername</b> <code>%UserName%</code> ein. Wenn der Proxy-Server den Domännennamen zur Authentifizierung benötigt, verwenden Sie das Format <code>&lt;domäne&gt;\&lt;benutzername&gt;</code>.</li> <li>2. Klicken Sie in der Dropdown-Liste <b>Benutzerdefinierbar</b> auf die Proxy-Einstellungen, die die Benutzer von BlackBerry 10-Geräten ändern können. Die Standardeinstellung ist <b>Schreibgeschützt</b>.</li> </ol> </li> </ol>
Festlegen der Einstellungen zur manuellen Konfiguration	<ol style="list-style-type: none"> <li>a. Klicken Sie in der Dropdown-Liste <b>Typ</b> auf <b>Manuelle Konfiguration</b>.</li> <li>b. Geben Sie im Feld <b>Host</b> den FQDN oder die IP-Adresse des Proxy-Servers ein.</li> <li>c. Geben Sie im Feld <b>Port</b> die Portnummer des Proxy-Servers ein.</li> <li>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 <b>Benutzername</b> <code>%UserName%</code> ein. Wenn der Proxy-Server den Domännennamen zur Authentifizierung benötigt, verwenden Sie das Format <code>&lt;domäne&gt;\&lt;benutzername&gt;</code>.</li> <li>e. Führen Sie auf der Registerkarte <b>BlackBerry</b> die folgenden Aktionen aus: <ol style="list-style-type: none"> <li>1. Klicken Sie in der Dropdown-Liste <b>Benutzerdefinierbar</b> auf die Proxy-Einstellungen, die die Benutzer von BlackBerry 10-Geräten ändern können. Die Standardeinstellung ist <b>Schreibgeschützt</b>.</li> <li>2. Optional können Sie eine Liste der Adressen festlegen, auf die die Benutzer über ihre BlackBerry 10-Geräte direkt zugreifen können, ohne dazu den Proxy-Server zu verwenden. Geben Sie im Feld <b>Ausschlussliste</b> die Adressen (FQDN oder IP) ein, und trennen Sie die einzelnen Werte in der Liste mit einem Semikolon (;). Sie können das Platzhalterzeichen (*) in einem FQDN oder einer IP-Adresse (z. B. <code>*.beispiel.com</code> oder <code>192.0.2.*</code>) verwenden.</li> </ol> </li> </ol>

7. Wiederholen Sie die Schritte 4 und 5 für jeden Gerätetyp in Ihrer Organisation.

8. Klicken Sie auf **Hinzufügen**.

**Wenn Sie fertig sind:**

- Verknüpfen Sie das Proxy-Profil mit einem Wi-Fi-, VPN- oder Enterprise-Konnektivitätsprofil.
- Legen Sie ggf. eine Rangfolge für die Profile fest. Die von Ihnen festgelegte Reihenfolge gilt nur, wenn Sie den Benutzergruppen oder Gerätegruppen ein Proxy-Profil zuweisen.

# 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- und BlackBerry 10-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-Geräten können Sie zulassen, dass alle Apps den Tunnel nutzen oder festlegen, welche Apps „Per App VPN“ 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 auf iOS-Geräten „Per App VPN“ für BlackBerry Secure Connect Plus 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 UEM mit BlackBerry Infrastructure. Für jedes Gerät wird ein Tunnel erstellt. Der Tunnel unterstützt Standard-IPv4-Protokolle (TCP und UDP), und der IP-Datenverkehr, der zwischen Geräten und BlackBerry 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.

Weitere Informationen darüber, wie BlackBerry Secure Connect Plus Daten zu und von Geräten überträgt, finden Sie in der [Dokumentation zur lokalen Architektur](#) oder in der [Dokumentation zur Cloud-Architektur](#).

## Schritte zum Aktivieren von BlackBerry Secure Connect Plus

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

Schritt	Aktion
1	Stellen Sie sicher, dass die BlackBerry UEM-Domäne im Unternehmen die Anforderungen zur Verwendung von BlackBerry Secure Connect Plus erfüllt.

Schritt	Aktion
2	Wenn Sie über BlackBerry UEM Cloud verfügen, müssen Sie den BlackBerry Connectivity Node installieren oder BlackBerry Connectivity Node auf die neueste Version aktualisieren.
3	Aktivieren Sie BlackBerry Secure Connect Plus im Standard-Enterprise-Konnektivitätsprofil oder in einem von Ihnen erstellten benutzerdefinierten Enterprise-Konnektivitätsprofil.
4	Optional: Legen Sie die DNS-Einstellungen für die BlackBerry Connectivity-App fest.
5	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.
6	Weisen Sie das Enterprise-Konnektivitätsprofil <a href="#">Benutzerkonten</a> oder <a href="#">Benutzergruppen</a> 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:

- Die Firewall muss ausgehende Verbindungen über Port 3101 mit `<Region>.turnb.bbsecure.com` und `<Region>.bbsecure.com` zulassen. Wenn Sie BlackBerry UEM zur Verwendung eines Proxyservers konfigurieren, muss dieser Verbindungen über Port 3101 mit diesen Unterdomänen zulassen. Weitere Informationen zu den Domänen und IP-Adressen für die Firewall-Konfiguration finden Sie unter <http://support.blackberry.com/community> in Artikel 36470.
- In jeder BlackBerry 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 über BlackBerry UEM Cloud verfügen, müssen Sie [den BlackBerry Connectivity Node installieren oder ihn auf die neueste Version aktualisieren](#).

**Hinweis:** Wenn in Ihrer lokalen 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](#).

**Hinweis:** Wenn Sie ein E-Mail-Profil zum Aktivieren von BlackBerry Secure Gateway für iOS-Geräte verwenden, empfiehlt sich die Konfiguration von „Per App VPN“ für BlackBerry Secure Connect Plus. Weitere Informationen zum BlackBerry Secure Gateway finden Sie unter [Schützen von E-Mail-Daten mithilfe von BlackBerry Secure Gateway](#).

## Unterstützte Geräte:

Gerät	Anforderungen
iOS	<ul style="list-style-type: none"><li>• Geräte müssen mit dem BlackBerry UEM Client aus dem App Store aktiviert werden.</li><li>• MDM-Steurelemente-Aktivierungstyp</li></ul>
Android Enterprise	<ul style="list-style-type: none"><li>• Eine der folgenden Aktivierungsarten:<ul style="list-style-type: none"><li>• Nur geschäftlicher Bereich (Premium)</li><li>• Geschäftlich und persönlich – vollständige Kontrolle (Premium)</li><li>• Geschäftlich und persönlich – Benutzer-Datenschutz (Premium)</li></ul></li></ul>
Samsung Knox Workspace	<ul style="list-style-type: none"><li>• Samsung Knox MDM Version 5.0 oder höher</li><li>• Samsung Knox Version 2.3 oder höher</li><li>• Eine der folgenden Aktivierungsarten:<ul style="list-style-type: none"><li>• Nur geschäftlicher Bereich (Samsung Knox)</li><li>• Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)</li><li>• Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)</li></ul></li></ul>
BlackBerry 10	<ul style="list-style-type: none"><li>• BlackBerry 10 OS Version 10.3.2 oder höher</li><li>• Eine der folgenden Aktivierungsarten:<ul style="list-style-type: none"><li>• Geschäftlich und persönlich – Unternehmen</li><li>• Nur geschäftlicher Bereich</li><li>• Geschäftlich und persönlich – Reguliert</li></ul></li></ul>

## Installieren zusätzlicher BlackBerry Secure Connect Plus-Komponenten in einer lokalen Umgebung

Sie können eine oder mehrere Instanzen des BlackBerry Connectivity Node installieren, um weitere Instanzen der Geräteverbindungskomponenten zur Domäne Ihres Unternehmens hinzuzufügen. Jeder BlackBerry Connectivity Node enthält eine aktive Instanz von BlackBerry Secure Connect Plus zur Verarbeitung von Gerätedaten und zum Aufbau sicherer Verbindungen.

Sie können auch Servergruppen erstellen. Eine Servergruppe enthält eine oder mehrere Instanzen des BlackBerry Connectivity Node. Beim Erstellen einer Servergruppe geben Sie den regionalen Datenpfad an, den die zu verwendenden Komponenten für die Verbindung mit der BlackBerry Infrastructure nutzen sollen. Sie können beispielsweise eine Servergruppe erstellen, um Geräteverbindungen für BlackBerry Secure Connect Plus und BlackBerry Secure Gateway so zu lenken, dass der Pfad für die USA zur BlackBerry Infrastructure verwendet wird. Sie können E-Mail- und Enterprise-Konnektivitätsprofile mit einer Servergruppe verknüpfen. Jedes Gerät, dem diese Profile zugewiesen wurden, nutzt die regionale Verbindung dieser Servergruppe zur BlackBerry Infrastructure, wenn Komponenten der BlackBerry Connectivity Node verwendet werden.

Wenn es in einer Domäne mehrere BlackBerry UEM-Instanzen gibt, wird die BlackBerry Secure Connect Plus-Komponente in jeder Instanz ausgeführt und verarbeitet Daten. Für die Daten erfolgt eine Lastverteilung über alle BlackBerry Secure Connect Plus-Komponenten in der Domäne.

Failover für hohe Verfügbarkeit ist für BlackBerry Secure Connect Plus verfügbar. Wenn ein Gerät einen sicheren Tunnel verwendet und die aktuelle BlackBerry Secure Connect Plus-Komponente unverfügbar wird, weist die BlackBerry Infrastructure das Gerät einer BlackBerry Secure Connect Plus-Komponente in einer anderen BlackBerry UEM-Instanz zu. Das Gerät nimmt die Verwendung des sicheren Tunnels mit minimaler Unterbrechung wieder auf.

Weitere Informationen zum Planen und Installieren eines BlackBerry Connectivity Node [finden Sie in der Dokumentation zur Planung](#) und [in der Dokumentation zu Installation und Upgrade](#).

## Installieren oder Aktualisieren der BlackBerry Secure Connect Plus-Komponente in einer Cloud-Umgebung

Wenn Sie BlackBerry Connectivity Node installieren, wird beim Einrichtungsvorgang auch die BlackBerry Secure Connect Plus-Komponente auf dem gleichen Computer installiert. Wenn Sie ein Upgrade von BlackBerry Connectivity Node auf die neueste Version ausführen, und BlackBerry Secure Connect Plus nicht installiert ist, wird beim Upgradeprozess BlackBerry Secure Connect Plus installiert. Wenn BlackBerry Secure Connect Plus zuvor bereits installiert war, erfolgt ein Upgrade von BlackBerry Secure Connect Plus auf die neueste Version.

Anweisungen zu Installation oder Upgrade von BlackBerry Connectivity Node [finden Sie unter „Installation und Upgrade von BlackBerry Connectivity Node“ in der BlackBerry UEM Cloud Dokumentation zur Konfiguration](#). Sie müssen BlackBerry Connectivity Node aktivieren, bevor Sie BlackBerry Secure Connect Plus aktivieren können.

Sie haben die Möglichkeit, die Daten, die zwischen BlackBerry Secure Connect Plus und der BlackBerry Infrastructure übertragen werden, über den BlackBerry Router oder einen TCP-Proxyserver (transparent oder SOCKS v5) zu leiten. Sie können die Proxyeinstellungen über die BlackBerry Connectivity Node-Verwaltungskonsole (Allgemeine Einstellungen > Proxy) konfigurieren.

**Hinweis:** Wenn Sie ungültige Proxyinformationen angeben, wird BlackBerry Secure Connect Plus nicht weiter ausgeführt und kann nicht neu gestartet werden. Wenn dieses Problem auftritt, korrigieren Sie die Proxyinformationen, und starten Sie den BlackBerry UEM – BlackBerry Secure Connect Plus-Dienst in den Windows Services neu.

Sie können einen zweiten BlackBerry Connectivity Node für Redundanz installieren. Auf beiden Instanzen von BlackBerry Secure Connect Plus werden Daten ausgeführt und verarbeitet. Die Lastverteilung der Daten erfolgt über beide Instanzen hinweg. Wenn ein Gerät einen sicheren Tunnel verwendet und die aktuelle BlackBerry Secure Connect Plus-Instanz nicht mehr verfügbar ist, weist die BlackBerry Infrastructure das Gerät der anderen Instanz zu. Das Gerät nimmt die Verwendung des sicheren Tunnels mit minimaler Unterbrechung wieder auf.

## BlackBerry Secure Connect Plus aktivieren

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-Geräten wird die App automatisch aus dem App Store installiert). Auf BlackBerry 10-Geräten ist die App verborgen und erfordert keine Benutzerinteraktion.

BlackBerry veröffentlicht zur Unterstützung neuer Funktionen und Verbesserungen neue Versionen der App. Anweisungen zum Upgrade der App und Informationen zu den neuesten bekannten und behobenen Fehlern finden Sie in den [BlackBerry Connectivity-App-Versionshinweisen](#).

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

2. Klicken Sie auf **Netzwerke und Verbindungen > Enterprise-Konnektivität**.
3. Klicken Sie auf **+**.
4. 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.
5. Konfigurieren Sie die entsprechenden Werte für die Profileinstellungen jedes Gerätetyps. Weitere Informationen zu den Profileinstellungen finden Sie unter [Enterprise-Konnektivitätsprofileinstellungen](#).
6. Klicken Sie auf **Hinzufügen**.
7. Weisen Sie das Profil Benutzergruppen bzw. Benutzerkonten zu.
8. Wenn Sie „Per App VPN“ für iOS-Geräte konfiguriert haben, verknüpfen Sie dies mit dem entsprechenden Enterprise-Konnektivitätsprofil, wenn Sie eine App oder App-Gruppe zuweisen.

**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. Die Benutzer von iOS-, Android Enterprise- und Knox Workspace-Geräten können die App zum Anzeigen des Status der Verbindung öffnen. Es sind keine weiteren Maßnahmen von den Benutzern erforderlich.
- Wenn Sie mehrere Enterprise-Konnektivitäts-Profile erstellt haben, weisen Sie ihnen eine Rangordnung zu.
- Wenn Sie ein Verbindungsproblem mit einem iOS-, 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.
- 

**Enterprise-Konnektivitätsprofileinstellungen**

[Enterprise-Konnektivitätsprofile](#) werden auf den folgenden Gerätetypen unterstützt:


- iOS
- Android
- BlackBerry 10

**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.  Diese Einstellung ist nur gültig, wenn Sie eine oder mehrere Instanzen von BlackBerry Connectivity Node installiert und Servergruppen eingerichtet haben.



## iOS: Enterprise-Konnektivitätsprofileinstellungen

Einstellung	Beschreibung
BlackBerry Secure Connect Plus aktivieren	Diese Einstellung gibt an, ob geschäftliche Apps BlackBerry Secure Connect Plus für das Senden von geschäftlichen Daten zwischen Geräten und Ihrem Netzwerk verwenden.
VPN bei Bedarf aktivieren	Diese Einstellung legt fest, ob eine geschäftliche App automatisch eine VPN-Verbindung mittels BlackBerry Secure Connect Plus starten kann, wenn sie Zugriff auf geschäftliche Ressourcen hat.  Wählen Sie diese Einstellung, um Regeln für BlackBerry Secure Connect Plus-Verbindungen festzulegen.
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	Wählen Sie diese Einstellung, um nur bestimmten Apps die Nutzung von BlackBerry Secure Connect Plus zu gestatten.  <b>Hinweis:</b> 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, wann es angebracht ist, die VPN-Verbindung ein- bzw. auszuschalten (die VPN-Verbindung kann beispielsweise aktiviert werden, wenn Benutzer sich nicht im Abdeckungsbereich des geschäftlichen Wi-Fi-Netzwerks aufhalten).
Safari-Domänen	Wenn Sie die Domänen angeben möchten, die eine VPN-Verbindung in Safari starten dürfen, klicken Sie auf  .
Zulassen, dass Apps automatisch eine Verbindung herstellen	Legen Sie fest, ob Apps die VPN-Verbindung automatisch initiieren können.
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 <a href="#">Einrichten von Proxy-Profilen für Geräte</a> .

## Android: Enterprise-Konnektivitätsprofileinstellungen

Einstellung	Beschreibung
BlackBerry Secure Connect Plus aktivieren	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	<p>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.</p> <ul style="list-style-type: none"> <li>• „Containerweites VPN“ verwendet eine VPN-Verbindung für alle Apps im geschäftlichen Bereich auf dem Gerät.</li> <li>• „Per App VPN“ verwendet nur für die angegebenen Apps eine VPN-Verbindung.</li> </ul>
Apps, die BlackBerry Secure Connect Plus nicht verwenden dürfen	<p>Diese Einstellung gibt Apps im geschäftlichen Bereich auf Android Enterprise-Geräten an, die BlackBerry Secure Connect Plus nicht verwenden dürfen.</p> <p>Klicken Sie auf <b>+</b>, und geben Sie die App-Paket-ID ein. Wiederholen Sie den Vorgang bei Bedarf, um weitere Apps zu sperren.</p> <p>Google Play und die zugrunde liegenden Dienste (com.android.providers.media, com.android.vending, com.google.android.gms und com.google.android.apps.gcs) sind standardmäßig gesperrt, da Google Play keine Proxyverbindungen unterstützt. Es wird empfohlen, diese Einschränkungen beizubehalten. Wenn Sie eine dieser 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.</p> <p>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 BlackBerry UEM Client mit BlackBerry Infrastructure über BlackBerry UEM kommunizieren kann. Weitere Informationen zum Öffnen von Ports in der Firewall, wenn geschäftliche Apps BlackBerry Secure Connect Plus verwenden, finden Sie unter <a href="http://support.blackberry.com/community">support.blackberry.com/community</a> im Artikel 48330.</p> <p>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 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.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Containerweites VPN“ gesetzt ist.</p>

Einstellung	Beschreibung
Apps, die Enterprise-Konnektivität verwenden dürfen	<p>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.</p> <p>Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Per App VPN“ gesetzt ist.</p>
Proxyprofil	<p>Wenn Sie Datenverkehr über einen sicheren Tunnel von Samsung Knox-Geräten mit Android Enterprise-Aktivierungen und Samsung Knox Workspace 2.5 oder höher über einen Proxyserver zum geschäftlichen Netzwerk weiterleiten möchten, wählen Sie das entsprechende Proxy-Profil aus.</p> <p>Diese Einstellung gilt nicht für Android Enterprise-Geräte, bei denen es sich nicht um Samsung Knox handelt, oder für Geräte mit Samsung Knox Workspace bis einschließlich Version 2.4.</p>

### BlackBerry 10: Enterprise-Konnektivitätsprofileinstellungen

Einstellung	Beschreibung
Enterprise-Konnektivität	Für BlackBerry 10-Geräte ist die Enterprise-Konnektivität immer aktiviert. Sie können diese Einstellung nicht ändern. Weitere Informationen finden Sie unter <a href="#">Verwaltung der Enterprise-Konnektivität für BlackBerry 10-Geräte</a> .
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.
BlackBerry Secure Connect Plus aktivieren	Diese Einstellung gibt an, ob geschäftliche Apps BlackBerry Secure Connect Plus für das Senden von geschäftlichen Daten zwischen Geräten und Ihrem Netzwerk verwenden.

## 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. Sie können außerdem Suffixe für die DNS-Suche angeben. Wenn Sie keine DNS-Einstellungen festlegen, bezieht die App DNS-Adressen von dem Computer, der die BlackBerry Secure Connect Plus-Komponente hostet, und als standardmäßiger Suchsuffix wird die DNS-Domäne dieses Computers verwendet.


Wenn Sie Servergruppen erstellen und konfigurieren, die BlackBerry Secure Connect Plus-Verbindungen zu einem bestimmten regionalen Pfad an die BlackBerry Infrastructure weiterleiten sollen, können Sie DNS-Einstellungen für die jeweilige Servergruppe festlegen. In diesem Fall erhalten die DNS-Einstellungen, die für eine Servergruppe gelten, Priorität über die globalen DNS-Einstellungen, die Sie mithilfe der folgenden Schritte konfigurieren. Weitere Informationen zum Erstellen und Konfigurieren von Servergruppen finden Sie in der [Dokumentation zur Installation und zum Upgrade lokaler Umgebungen](#) oder in der [Dokumentation zur Konfiguration von UEM Cloud](#).

1. Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie bei einer lokalen Umgebung in der UEM-Verwaltungskonsolle 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-Geräten oder Samsung Knox Workspace-Geräten installiert sind, sollten Sie die den Geräten zugewiesenen BlackBerry Dynamics-Konnektivitätsprofils 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 auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > BlackBerry Dynamics-Verbindungen**.
3. Wählen Sie aus, welches Profil Android Enterprise- und Samsung Knox Workspace-Geräten zugewiesen werden soll.
4. Klicken Sie auf .
5. Deaktivieren Sie das Kontrollkästchen **Sämtlichen Datenverkehr weiterleiten**.
6. Klicken Sie auf **Speichern**.


## Leiten des geschäftlichen Datenverkehrs in BlackBerry 10 über BlackBerry Secure Connect Plus, wenn ein Wi-Fi-Netzwerk verfügbar ist

Wenn Sie mit BlackBerry UEM ein Wi-Fi-Profil konfigurieren und BlackBerry 10-Geräten zuweisen, wird auf den Geräten dem geschäftlichen Wi-Fi-Netzwerk Vorrang vor BlackBerry Secure Connect Plus gegeben. Steht das geschäftliche Wi-Fi-Netzwerk nicht zur Verfügung, und den Geräten ist kein VPN-Profil zugewiesen oder sie haben keinen VPN-Zugriff, wird BlackBerry Secure Connect Plus verwendet. Sie können den gesamten geschäftlichen Datenverkehr über BlackBerry Secure Connect Plus leiten, selbst wenn Geräte Zugriff auf das geschäftliche Wi-

Fi-Netzwerk haben. Sie können diese Option verwenden, wenn die Sicherheitsstandards Ihres Unternehmens Geräteverbindungen zu geschäftlichen Ressourcen über das Wi-Fi-Netzwerk verhindern.

**Hinweis:** Bei Aktivierung dieser Funktion wird der gesamte Datenverkehr des geschäftlichen Bereichs, für den in der Regel das geschäftliche Wi-Fi-Netzwerk verwendet würde, über eine sichere Verbindung zur BlackBerry Infrastructure weitergeleitet. Diese Funktion kann Auswirkungen auf Datennutzungs- und Netzwerkkosten Ihres Unternehmens haben. Vergewissern Sie sich, dass dies die bevorzugte Konfiguration im Unternehmen ist, bevor Sie diese Funktion aktivieren.

**Bevor Sie beginnen:** Stellen Sie in lokalen Umgebungen sicher, dass die IT-Richtlinienregel „Steuerung des Netzwerkzugriffs für geschäftliche Apps erzwingen“ nicht in der IT-Richtlinie ausgewählt ist, die BlackBerry 10-Gerätebenutzern zugewiesen ist.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > WLAN**.
3. Klicken Sie auf ein Wi-Fi-Profil, das BlackBerry 10-Gerätebenutzern zugewiesen ist.
4. Klicken Sie auf .
5. Aktivieren Sie auf der Registerkarte **BlackBerry** im Bereich **Verknüpfte Profile** das Kontrollkästchen **Enterprise-Konnektivitäts-Profil mit BlackBerry Secure Connect Plus-Verbindung für geschäftliche Daten verwenden**.
6. Klicken Sie auf **Speichern**.

**Wenn Sie fertig sind:** Wenn Sie mehrere Wi-Fi-Profile erstellt und zugewiesen haben, wiederholen Sie diese Schritte entsprechend.

## 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-Adapter wechselt in den Zustand „Nicht identifiziertes Netzwerk“ und funktioniert nicht mehr**

#### **Ursache**

Dieses Problem kann auftreten, wenn Sie den Computer, auf dem BlackBerry Secure Connect Plus gehostet wird, neu starten.

#### **Lösung für Windows Server 2012**

1. Klicken Sie im Server-Manager auf **Verwalten > Rollen und Features hinzufügen**. Klicken Sie so oft auf **Weiter**, bis der Bildschirm **Features** angezeigt wird. Erweitern Sie **Remoteserver-Verwaltungstools > Rollenverwaltungstools**, und wählen Sie **Tools für die Remotezugriffsverwaltung**. Schließen Sie den Assistenten zum Installieren der Tools ab.
2. Klicken Sie auf **Extras > Remotezugriffsverwaltung**.
3. Klicken Sie unter **Konfiguration** auf **DirectAccess und VPN**.
4. Klicken Sie unter **VPN** auf **RRAS-Verwaltung öffnen**.
5. Klicken Sie mit der rechten Maustaste auf den Routing- und RAS-Server und dann auf **Routing und RAS deaktivieren**.
6. Klicken Sie mit der rechten Maustaste auf den Routing- und RAS-Server und dann auf **Routing und RAS konfigurieren und aktivieren**.
7. Schließen Sie den Setup-Assistenten unter Auswahl folgender Optionen ab:

- a. Wählen Sie im Bildschirm **Konfiguration** die Option **Netzwerkadressenübersetzung (NAT)**.
- b. Wählen Sie im Bildschirm **NAT-Internetverbindung** die Option **Diese öffentliche Schnittstelle zum Herstellen der Internetverbindung verwenden**. Vergewissern Sie sich, dass BlackBerry Secure Connect Plus in der Liste der Netzwerkschnittstellen angezeigt wird.
8. Öffnen Sie **Weiterleitung und Remote-Zugriff** > <Servername> > **IPv4**, und klicken Sie auf **NAT**. Öffnen Sie die Eigenschaften von **LAN-Verbindung**, und wählen Sie **An das Internet angeschlossene, öffentliche Schnittstelle** und **NAT auf dieser Schnittstelle aktivieren**. Klicken Sie auf **OK**.
9. Öffnen Sie die Eigenschaften von **BlackBerry Secure Connect Plus**, und wählen Sie **An ein privates Netzwerk angeschlossene, private Schnittstelle**. Klicken Sie auf **OK**.
10. Klicken Sie mit der rechten Maustaste auf den Routing- und RAS-Server und dann auf **Alle Tasks** > **Neu starten**.
11. Starten Sie in den Windows-Diensten den Dienst **BlackBerry UEM – BlackBerry Secure Connect Plus** neu.

Laden und installieren Sie den Hotfix im Windows-KB-Artikel [NAT functionality fails on a Windows Server 2012-based RRAS server](#).

## 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 BlackBerry 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 <Laufwerk>:\Program Files\BlackBerry\UEMSecureConnectPlus\config\blackberry\, und führen Sie **configureRRAS.bat** aus.
5. Navigieren Sie zu <Laufwerk>:\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**

Zwei Protokolldateien mit Standardspeicherort <Laufwerk>:\Program Files\BlackBerry\UEM\Logs\<jjjmmmtt> erfassen Daten zu BlackBerry Secure Connect Plus:

- BSCP: Protokolldaten zur BlackBerry Secure Connect Plus-Serverkomponente
- BSCP-TS: Protokolldateien zu Verbindungen mit der BlackBerry Connectivity-App

Auf jedem Computer, der eine BlackBerry Connectivity Node-Instanz hostet, befinden sich die Protokolldateien für BlackBerry Secure Connect Plus unter <Laufwerk>:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs\<JJJMMTT>.

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 der Enterprise-Konnektivität für BlackBerry 10-Geräte

Die Enterprise-Konnektivität sendet alle geschäftlichen, zwischen BlackBerry 10-Geräten und dem Netzwerk Ihres Unternehmens gesendeten Daten über die BlackBerry Infrastructure an BlackBerry UEM. Enterprise-Konnektivität wird nur unterstützt, wenn BlackBerry UEM in einer lokalen Umgebung installiert ist. Durch diese Funktion wird vermieden, eine direkte Internetverbindung über die Firewall Ihres Unternehmens für die BlackBerry 10-Geräteverwaltung und Apps zu öffnen, die Verbindungen zu Ihrem E-Mail-Server, internen Zertifizierungsstellen und anderen Web- oder Inhaltsservern aufbauen. Bei BlackBerry 10-Geräten ist die Enterprise-Konnektivität immer aktiviert, auch wenn Sie BlackBerry Secure Connect Plus nicht verwenden. BlackBerry 10-Geräte wählen je nach Netzwerkverfügbarkeit den effizientesten Weg, um eine Verbindung zu Ihren geschäftlichen Ressourcen herzustellen.

Sie können ein [Proxyprofil](#) mit einem Enterprise-Konnektivitätsprofil verknüpfen, um Daten über einen Proxyserver zu senden.

Weitere Informationen darüber, wie BlackBerry 10-Geräte Daten über die Enterprise-Konnektivität in das und aus dem Netzwerk Ihres Unternehmens übertragen, finden Sie in der [Dokumentation zur lokalen Architektur](#).

## Verwaltung der Enterprise-Konnektivität für BlackBerry 10-Geräte

Wenn Sie ein Enterprise-Konnektivitätsprofil zur Konfiguration von BlackBerry Secure Connect Plus verwenden möchten, sehen Sie sich stattdessen [BlackBerry Secure Connect Plus aktivieren](#) an.

BlackBerry UEM weist allen Benutzern standardmäßig das Standardprofil für die Enterprise-Konnektivität zu. Sie können das Standardprofil bearbeiten oder neue Enterprise-Konnektivitätsprofile erstellen.

Auf BlackBerry 10-Geräten ist die Enterprise-Konnektivität immer aktiviert. Sie können das Enterprise-Konnektivitätsprofil verwenden, um ein Proxyprofil zum Senden von Daten über einen Proxy-Server zu verknüpfen.

**Bevor Sie beginnen:** Erstellen Sie bei Bedarf ein Proxyprofil.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > Enterprise-Konnektivität**.
3. Klicken Sie auf **+**.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein. Jedes Enterprise-Konnektivitätsprofil muss über einen eindeutigen Namen verfügen.
5. Klicken Sie auf die Registerkarte **BlackBerry**.
6. Wenn Sie einen Proxy-Server verwenden möchten, wählen Sie ein Proxy-Profil aus.
7. Klicken Sie auf **Hinzufügen**.

**Wenn Sie fertig sind:** Legen Sie ggf. eine Rangfolge für die Profile fest.



# 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-Verwaltungskonsolle, 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](#).

# Einrichten einer Authentifizierung bei einmaliger Anmeldung für Geräte

Mithilfe einer einmaligen Anmeldung können Sie es BlackBerry 10-Geräten und bestimmten iOS-Geräten ermöglichen, sich bei Domänen und Webdiensten Ihres Unternehmensnetzwerks automatisch zu authentifizieren. Nach Zuweisung einer einmaligen Anmeldung 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.

Auf Geräten mit iOS (oder iPadOS) 13 oder höher müssen Sie ein Profil für die Single-Sign-On-Erweiterung verwenden, damit sich die Geräte automatisch bei Domänen und Webservices im Netzwerk Ihres Unternehmens authentifizieren können.

Sie können auch mithilfe eines Profils für die einmalige Anmeldung vertrauenswürdige Domänen für Zertifikate angeben, die Sie mit einem SCEP-Profil an BlackBerry 10-Geräte senden. Wenn Sie vertrauenswürdige Domänen festlegen, können BlackBerry 10-Benutzer die erforderlichen Zertifikate beim Zugriff auf eine vertrauenswürdige Domäne auswählen.

Profile für die einmalige Anwendung unterstützen die folgenden Authentifizierungstypen:

Authentifizierungstyp	Geräte-OS	Gilt für
• Kerberos	iOS	• Browser und Apps • Kann einschränken, von welchen Apps das Profil verwendet werden kann
	BlackBerry 10	• Browser und Apps im geschäftlichen Bereich
• NTLM • Festlegen vertrauenswürdiger Domänen für SCEP-Zertifikate	BlackBerry 10	• Browser und Apps im geschäftlichen Bereich

BlackBerry Dynamics-Apps unterstützen auch die Kerberos-Authentifizierung. Weitere Informationen finden Sie unter [Konfigurieren von Kerberos für BlackBerry Dynamics-Apps](#).

## Voraussetzungen: Verwenden der Kerberos-Authentifizierung für Geräte

Bei der Verwendung von Kerberos mit Geräten, wenn eine gültige TGT auf den Geräten verfügbar ist, werden Benutzer nicht zur Eingabe der Anmeldeinformationen aufgefordert, wenn sie mithilfe des Browsers und der Apps im geschäftlichen Bereich auf die internen Ressourcen Ihres Unternehmens zugreifen.

Zur Konfiguration der Kerberos-Authentifizierung für bestimmte Domänen können Sie die Kerberos-Konfigurationsdatei Ihrer Organisation (krb5.conf) hochladen. BlackBerry UEM unterstützt die Heimdal-Implementierung von Kerberos.

Stellen Sie sicher, dass die Konfigurationsdatei die folgenden Anforderungen erfüllt:

- Die Kerberos-Konfiguration muss standardmäßig TCP anstelle von UDP verwenden. Verwenden Sie das Präfix tcp/ für KDC-Hosts.
- Wenn Ihre Organisation VPN verwendet, muss der VPN-Gateway Verkehr zu den KDCs zulassen.

## Zertifikatbasierte Authentifizierung für iOS-Geräte

Bei iOS-Geräten können Sie Zertifikate zum Authentifizieren von Geräten mit Domänen und Webdiensten in Ihrem Unternehmensnetzwerk verwenden. Sie können einem Profil zur einmaligen Anmeldung ein freigegebenes Zertifikatprofil, ein SCEP-Profil oder ein Profil für Benutzeranmeldeinformationen hinzufügen. Wenn der Browser oder die Apps auf iOS-Geräten die zertifikatbasierte einmalige Anmeldung verwenden, werden die Benutzer automatisch authentifiziert (solange das Zertifikat gültig ist). Sie müssen keine Anmeldeinformationen eingeben, wenn sie auf die von Ihnen festgelegten sicheren Domänen zugreifen.

## Erstellen eines Profils für die einmalige Anmeldung

Profile für die einmalige Anmeldung werden für BlackBerry 10- und iOS-Geräte unterstützt. Informationen zum Einrichten der Authentifizierung mit einmaliger Anmeldung für BlackBerry Dynamics-Apps finden Sie unter [Kerberos für BlackBerry Dynamics-Apps konfigurieren](#).

### Bevor Sie beginnen:

- Wenn Sie die Kerberos-Authentifizierung für BlackBerry 10-Geräte konfigurieren möchten, suchen Sie die Kerberos-Konfigurationsdatei Ihrer Organisation (krb5.conf).
  - Wenn Sie die zertifikatbasierte Authentifizierung für iOS-Geräte verwenden möchten, erstellen Sie das erforderliche Profil für ein freigegebenes Zertifikat oder das SCEP-Profil.
1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
  2. Klicken Sie auf **Netzwerke und Verbindungen > Single-Sign-on**.
  3. Klicken Sie auf **+**.
  4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
  5. Führen Sie eine der folgenden Aufgaben aus:

Aufgabe	Schritte
Konfigurieren der Kerberos-Authentifizierung für iOS-Geräte	<ol style="list-style-type: none"> <li>a. Klicken Sie auf die Registerkarte <b>iOS</b>.</li> <li>b. Klicken Sie unter <b>Kerberos</b> auf <b>+</b>.</li> <li>c. Geben Sie im Feld <b>Name</b> einen Namen für die Konfiguration ein.</li> <li>d. Geben Sie im Feld <b>Prinzipalname</b> den Namen des Kerberos-Prinzipals im Format <code>&lt;Primär&gt;/&lt;Instanz&gt;@&lt;Bereich&gt;</code> ein (z. B. <code>user/admin@blackberry.example.com</code>).</li> <li>e. Geben Sie im Feld <b>Bereich</b> den Kerberos-Bereich in Großbuchstaben (z. B. <b>EXAMPLE.COM</b>) ein.</li> <li>f. Geben Sie im Feld <b>URL-Präfixe</b> das URL-Präfix für die Websites ein, mit dem sich Geräte authentifizieren sollen. Das Präfix muss mit <code>http://</code> oder <code>https://</code> beginnen und kann Platzhalterwerte (*) enthalten (z. B. <b>https://www.blackberry.example.com/*</b>).</li> <li>g. Um mehr URL-Präfixe festzulegen, klicken Sie auf <b>+</b>, um weitere Felder hinzuzufügen.</li> <li>h. Wenn Sie die Konfiguration auf bestimmte Apps einschränken möchten, klicken Sie auf <b>+</b> neben <b>App-Bezeichner</b>. Geben Sie die App-Bundle-ID ein. Sie können einen Platzhalterwert (*) verwenden, um die ID mit mehreren Apps abzugleichen. (Z. B. <b>com.company.*</b>).</li> <li>i. Um mehr App-Bezeichner festzulegen, klicken Sie auf <b>+</b>, um weitere Felder hinzuzufügen.</li> <li>j. Wenn iOS-Geräte die zertifikatbasierte Authentifizierung verwenden sollen, klicken Sie in der Dropdown-Liste <b>Anmeldeinformationen</b> auf <b>Zertifikat</b>, <b>SCEP</b> oder <b>Benutzeranmeldeinformationen</b>. Klicken Sie in der Dropdown-Liste „Zertifikat“ auf das Zertifikatprofil, das Sie verwenden möchten.</li> <li>k. Klicken Sie auf <b>Hinzufügen</b>.</li> <li>l. Wiederholen Sie ggf. die Schritte 2 bis 11, um eine weitere Kerberos-Konfiguration hinzuzufügen.</li> </ol>
Konfigurieren der Kerberos-Authentifizierung für BlackBerry 10-Geräte	<ol style="list-style-type: none"> <li>a. Klicken Sie auf die Registerkarte <b>BlackBerry</b>.</li> <li>b. Klicken Sie auf <b>Durchsuchen</b>. Navigieren Sie zur Kerberos-Konfigurationsdatei Ihrer Organisation (<code>krb5.conf</code>), und wählen Sie diese aus.</li> </ol>

Aufgabe	Schritte
Konfigurieren der NTLM-Authentifizierung oder vertrauenswürdiger Domänen für SCEP-Zertifikate für BlackBerry 10-Geräte	<ol style="list-style-type: none"> <li>a. Klicken Sie auf die Registerkarte <b>BlackBerry</b>.</li> <li>b. Klicken Sie unter <b>Vertrauenswürdige Domänen</b> auf <b>+</b>.</li> <li>c. Geben Sie im Feld <b>Name</b> einen Namen für die Konfiguration ein.</li> <li>d. Geben Sie im Feld <b>Domäne</b> eine vertrauenswürdige Unterdomäne oder einen einzelnen Host ein, auf dem die Anmeldeinformationen für die Domäne zur automatischen Authentifizierung verwendet werden können. Geben Sie den Servernamen als einen FQDN, Hostnamen, Alias-Namen oder eine IP-Adresse ein. DNS-Namen können Platzhalter (*) enthalten.</li> <li>e. Um mehr Unterdomänen festzulegen, klicken Sie auf <b>+</b>, um weitere Felder hinzuzufügen.</li> <li>f. Klicken Sie auf <b>Hinzufügen</b>.</li> <li>g. Wiederholen Sie ggf. die Schritte 2 bis 6, um eine weitere vertrauenswürdige Domäne hinzuzufügen.</li> </ol>

6. Klicken Sie auf **Hinzufügen**.

**Wenn Sie fertig sind:** Legen Sie ggf. eine Rangfolge für die Profile fest.

## SSO-Erweiterungsprofil erstellen

Single Sign-On-Erweiterungen werden auf Geräten mit iOS und iPadOS 13 oder höher unterstützt.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > SSO-Erweiterung**.
3. Klicken Sie auf **+**.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie im Feld **Erweiterungs-ID** die Kennung für die App ein, die die einmalige Anmeldung durchführt.
6. Wählen Sie einen Anmeldestyp aus.

Aufgabe	Schritte
Wenn Sie <b>Anmeldeinformationen</b> auswählen:	<ol style="list-style-type: none"> <li>a. Geben Sie im Feld <b>Bereich</b> den Bereichsnamen für die Anmeldedaten ein.</li> <li>b. Klicken Sie im Abschnitt <b>Domänen</b> auf <b>+</b>, um eine Domäne hinzuzufügen.</li> <li>c. Geben Sie im Feld <b>Name</b> die Domäne ein, für die die App-Erweiterung die einmalige Anmeldung (Single Sign-On) durchführt.</li> <li>d. Fügen Sie nach Bedarf weitere Domänen hinzu.</li> <li>e. Geben Sie im Feld <b>Benutzerdefinierter Payload-Code</b> den benutzerdefinierten Payload-Code für die App-Erweiterung ein.</li> </ol>

Aufgabe	Schritte
Wenn Sie <b>Umleiten</b> auswählen:	<ul style="list-style-type: none"><li>a. Klicken Sie im Abschnitt <b>URLs</b> auf <b>+</b>, um eine URL hinzuzufügen.</li><li>b. Geben Sie im Feld <b>Name</b> 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.</li><li>c. Geben Sie im Feld <b>Benutzerdefinierter Payload-Code</b> den benutzerdefinierten Payload-Code für die App-Erweiterung ein.</li></ul>

7. Klicken Sie auf **Speichern**.

# Verwalten 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-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.

## Erstellen eines Profils für verwaltete Domänen

Profile für verwaltete Domänen gelten nur für iOS-Geräte.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > Verwaltete Domänen**.
3. Klicken Sie auf **+**.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
6. Klicken Sie im Abschnitt **Verwaltete E-Mail-Domänen** auf **+**.
7. Geben Sie im Feld **E-Mail-Domänen** einen Namen für eine Top-Level-Domäne ein (z. B. `beispiel.com` anstelle von `beispiel.com/canada`).
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie im Abschnitt **Verwaltete Webdomänen** auf **+**. Beispiele für Webdomänenformate [finden Sie unter „Managed Safari Web Domains“ in der iOS Developer Library](#).
10. Geben Sie im Feld **Webdomänen** den Namen einer Domäne ein.
11. 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 iOS-Geräte unterstützt.
12. Klicken Sie auf **Hinzufügen**.
13. Klicken Sie auf **Hinzufügen**.

# Kontrollieren der Netzwerknutzung von Apps auf iOS-Geräten

Sie können ein Netzwerknutzungsprofil verwenden, um zu steuern, wie die Apps auf iOS-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.

## Erstellen eines Netzwerknutzungsprofils

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 diese Benutzergruppen oder Benutzerkonten zu.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > Netzwerknutzung**.
3. Klicken Sie auf **+**.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Klicken Sie auf **+**.
6. 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 **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.\***).
7. Um zu verhindern, dass die App(s) Daten nutzen, wenn sich das Gerät im Roaming-Modus befindet, deaktivieren Sie das Kontrollkästchen **Datenroaming zulassen**.
8. Um zu verhindern, dass die App(s) Daten nutzen, wenn das Gerät mit dem mobilen Netzwerk verbunden ist, deaktivieren Sie das Kontrollkästchen **Mobile Daten zulassen**.
9. Klicken Sie auf **Hinzufügen**.
10. Wiederholen Sie Schritt 5 bis 9 für jede App, die Sie der Liste hinzufügen möchten.

**Wenn Sie fertig sind:** Legen Sie ggf. eine Rangfolge für die Profile fest.



# Filtern von Webinhalten 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-Gerät unter Aufsicht aufrufen kann. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen Webinhaltsfilter-Profile zuweisen.

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	<p>Diese Option erlaubt nur den Zugriff auf die von Ihnen festgelegten Websites. Für jede zugelassene Website wird in Safari ein Lesezeichen erstellt.</p> <p><b>Hinweis:</b> 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 <a href="#">moderne Authentifizierung von Microsoft Office 365 für BlackBerry Dynamics-Apps konfigurieren</a>, muss das Gerät die Active Directory Federation Services-Website erreichen können.</p>
Beschränken von nicht jugendfreien Inhalten	<p>Mit dieser Option werden unangemessene Inhalte automatisch erkannt und blockiert. Mit den folgenden Einstellungen können Sie auch bestimmte Websites einbinden:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>

## Erstellen von Webinhaltsfilter-Profilen

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).

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

Aufgabe	Schritte
Einrichten des Zugriffs auf lediglich bestimmte Websites	<ul style="list-style-type: none"> <li>a. Vergewissern Sie sich, dass in der Dropdown-Liste <b>Zugelassene Websites</b> die Option <b>Nur bestimmte Websites</b> ausgewählt ist.</li> <li>b. Klicken Sie im Abschnitt <b>Lesezeichen für bestimmte Websites</b> auf <b>+</b>.</li> <li>c. Führen Sie folgende Aktionen aus: <ul style="list-style-type: none"> <li>1. Geben Sie im Feld <b>URL</b> eine Webadresse ein, für die der Zugriff gestattet werden soll.</li> <li>2. Optional können Sie auch im Feld <b>Lesezeichenpfad</b> den Namen eines Lesezeichenordners eingeben (zum Beispiel: /Work/).</li> <li>3. Geben Sie im Feld <b>Titel</b> einen Namen für die Website ein.</li> <li>4. Klicken Sie auf <b>Hinzufügen</b>.</li> </ul> </li> <li>d. Wiederholen Sie die Schritte 2 und 3 für alle zugelassenen Websites.</li> </ul>
Beschränken von nicht jugendfreien Inhalten	<ul style="list-style-type: none"> <li>a. Klicken Sie in der Dropdown-Liste <b>Zugelassene Websites</b> auf <b>Nicht jugendfreie Inhalte beschränken</b>, um die automatische Filterung zu aktivieren.</li> <li>b. Führen Sie optional folgende Aktionen aus: <ul style="list-style-type: none"> <li>1. Klicken Sie auf <b>+</b> neben <b>Erlaubte URLs</b>.</li> <li>2. Geben Sie eine Webadresse ein, für die der Zugriff gewährt werden soll.</li> <li>3. Wiederholen Sie für jede zugelassene Website die Schritte 2.a und 2.b.</li> </ul> </li> <li>c. Führen Sie optional folgende Aktionen aus: <ul style="list-style-type: none"> <li>1. Klicken Sie auf <b>+</b> neben <b>Gesperrte URLs</b>.</li> <li>2. Geben Sie eine Webadresse ein, für die der Zugriff nicht gewährt werden soll.</li> <li>3. Wiederholen Sie für jede beschränkte Website die Schritte 3.a und 3.b.</li> </ul> </li> </ul>

6. Klicken Sie auf **Hinzufügen**.

# Konfigurieren von AirPrint- und AirPlay-Profilen 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 Bonjour AirPrint-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 iOS-Geräten zuweisen, damit Benutzer Drucker nicht manuell konfigurieren müssen.

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

Mit einem AirPlay-Profil können Sie Kennwörter für bestimmte AirPlay-Geräte festlegen, um sicherzustellen, dass nur autorisierte Benutzer darauf zugreifen können. Sie können auch eine Liste der zulässigen Zielgeräte erstellen, um sicherzustellen, dass überwachte iOS-Geräte sich nur mit den AirPlay-Geräten verbinden können, die Sie angeben. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen AirPlay-Profile zuweisen.

## Beispiel: Ein Kennwort für ein AirPlay-Gerät festlegen

Wenn Sie den Zugriff auf ein bestimmtes AirPlay-Gerät beschränken möchten, fügen Sie den Namen des Geräts hinzu, und legen Sie ein Kennwort fest. Benutzer von iOS-Geräten mit diesem AirPlay-Profil müssen das Kennwort eingeben, um Zugriff auf das AirPlay-Gerät zu erhalten. Beachten Sie, dass das Kennwort durch das AirPlay-Profil erforderlich wird, und nicht durch das AirPlay-Gerät selbst. Benutzer von iOS-Geräten, die nicht über ein AirPlay-Profil verfügen, können trotzdem auf das AirPlay-Gerät ohne Kennwort zugreifen.

## Beispiel: Erstellen einer Liste von AirPlay-Geräten für überwachte iOS-Geräte

Wenn Sie zulassen möchten, dass überwachte iOS-Geräte Inhalte nur auf bestimmte Geräte streamen, können Sie die Geräte-ID hinzufügen. Überwachte Geräte können nur Inhalte auf Geräte streamen, die Sie angeben. Geräte, die nicht überwacht sind, werden dadurch nicht beeinträchtigt.

## Erstellen eines AirPrint-Profiles

Sie können AirPrint-Profile konfigurieren und iOS-Geräten zuweisen, damit Benutzer Drucker nicht manuell konfigurieren müssen.

Weitere Informationen zum Bonjour-Protokoll und zum Drucken mit einer BlackBerry Dynamics-App finden Sie unter [support.blackberry.com/community](http://support.blackberry.com/community) in Artikel 40030.

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > AirPrint**.
3. Klicken Sie auf **+**.
4. Geben Sie einen Namen und eine Beschreibung für das AirPrint-Profil ein.
5. Klicken Sie im Abschnitt **AirPrint-Konfiguration** auf **+**.
6. Geben Sie in das Feld **IP-Adresse** die IP-Adresse für den Drucker oder AirPrint-Server ein.
7. Geben Sie in das Feld **Ressourcenpfad** den Ressourcenpfad des Druckers ein.

Der Ressourcenpfad des Druckers entspricht dem Parameter `rp` des `_ippes.tcp` Bonjour-Datensatzes.  
Beispiel:

- Drucker/<Druckerserie>
  - Drucker/<Druckermodell>
  - ipp/print
  - IPP\_Printer
8. Wenn AirPrint-Verbindungen über TLS gesichert werden, aktivieren Sie optional das Kontrollkästchen **TLS erzwingen**. Diese Einstellung wird von iOS 11.0 und höher unterstützt.
  9. Wenn sich der Port vom Standard für das Internet Printing Protocol unterscheidet, geben Sie optional die Portnummer in das Feld **Port** ein. Diese Einstellung wird von iOS 11.0 und höher unterstützt.
  10. Klicken Sie auf **Hinzufügen**.
  11. Klicken Sie auf **Hinzufügen**.

## Erstellen eines AirPlay-Profiles

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > AirPlay**.
3. Klicken Sie auf **+**.
4. Geben Sie einen Namen und eine Beschreibung für das AirPlay-Profil ein.
5. Klicken Sie auf **+** im Abschnitt **Zugelassene Zielgeräte**.
6. Geben Sie im Feld **Gerätename** den Namen des AirPlay-Geräts ein, das Sie hinzufügen möchten. Sie können den Namen des AirPlay-Geräts in den Geräteeinstellungen suchen, oder Sie können den Namen des Gerätes durch Tippen auf **Airplay** im Control Center eines iOS-Geräts suchen, wodurch eine Liste der verfügbaren AirPlay-Geräte in Ihrer Nähe aufgeführt wird.
7. Geben Sie in das Feld **Kennwort** ein Kennwort ein.
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf **+** im Abschnitt **Zugelassene Zielgeräte für Geräte unter Aufsicht**.
10. Geben Sie im Feld **Geräte-ID** die Geräte-ID für das AirPlay-Gerät ein, das Sie hinzufügen möchten. Sie können die Geräte-ID für das AirPlay-Gerät in den Geräteeinstellungen finden. Weitere Informationen über die Suche nach der Geräte-ID finden Sie in der Dokumentation für Ihr Apple-Produkt.
11. Klicken Sie auf **Hinzufügen**.

# Konfigurieren von Zugriffspunktnamen 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. Access Point Name-Profile werden von Geräten mit Android 9.0 und höher mit Nur geschäftlicher Bereich- und Geschäftlich und persönlich – vollständige Kontrolle-Aktivierung 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 die IT-Richtlinienregel „Gerät zur Verwendung der APN-Profileinstellungen zwingen“ in den Android Global-IT-Richtlinienregeln (alle Android-Geräte) aus.

## Erstellen eines APN-Profiles

**Bevor Sie beginnen:** Rufen Sie alle erforderlichen APN-Einstellungen vom Betreiber ab.

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

## 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.

Einstellungen für APN-Profil	Beschreibung
APN-Bitmaske	<p>Diese Einstellung legt die Datenkommunikationstypen fest, die diese APN-Konfiguration verwenden. Unterschiedliche Datenkommunikationstypen können unterschiedliche Konfigurationen verwenden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• Standard-Datenverkehr</li> <li>• MMS-Datenverkehr</li> <li>• SUPL-unterstütztes GPS</li> <li>• DUN-Datenverkehr</li> <li>• Datenverkehr mit hoher Priorität</li> <li>• FOTA-Portal des Netzbetreibers</li> <li>• IMS</li> <li>• CBS</li> <li>• IA Initial Attach APN</li> <li>• Emergency PDN</li> <li>• MCX (Mission Critical Service)</li> </ul>
Proxyadresse	<p>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.</p>
Proxy-Port	<p>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.</p>
MMSC	<p>Diese Einstellung legt das Multimedia Messaging Service Center (MMSC) für das Senden und Empfangen von MMS-Nachrichten fest.</p>
MMS-Proxyadresse	<p>Diese Einstellung legt den HTTP-Proxy für die Kommunikation mit dem MMSC zum Senden und Empfangen von MMS-Nachrichten fest.</p>
MMS-Proxyport	<p>Diese Einstellung legt den HTTP-Proxyport für die Kommunikation mit dem MMSC zum Senden und Empfangen von MMS-Nachrichten fest.</p>
Authentifizierungstyp	<p>Diese Einstellung gibt den für die Kommunikation verwendeten Authentifizierungstyp an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• NONE</li> <li>• PAP</li> <li>• CHAP</li> <li>• PAP oder CHAP</li> </ul>
Benutzername	<p>Wenn die Einstellung „Authentifizierungstyp“ auf einen anderen Wert als NONE festgelegt ist, geben Sie einen Benutzernamen an, wenn er für die Authentifizierung erforderlich ist.</p>

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	<p>Diese Einstellung legt fest, ob IPv4, IPv6 oder beide im Heimnetzwerk für Geräte aktiviert werden sollen, die IPv6-Netzwerke unterstützen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• IP</li> <li>• IPV6</li> <li>• IPV4V6</li> <li>• PPP</li> </ul>
Roaming-Protokoll	<p>Diese Einstellung legt fest, ob IPv4, IPv6 oder beides beim Roaming für Geräte aktiviert werden soll, die IPv6-Netzwerke unterstützen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• IP</li> <li>• IPV6</li> <li>• IPV4V6</li> <li>• PPP</li> </ul>
Betreiber-aktiviert	Diese Einstellung legt fest, ob der APN für den Betreiber aktiviert ist.
MVNO-Typ	<p>Diese Einstellung legt fest, ob die Nutzung dieses APN auf bestimmte MVNOs (Mobilfunknetzändler) oder Abonnementkonten beschränkt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• SP</li> <li>• IMSI</li> <li>• GID</li> <li>• ICCID</li> </ul>

# Rechtliche Hinweise

©2020 BlackBerry Limited. Sämtliche Marken, einschließlich, aber nicht beschränkt auf BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE und SECUSMART, sind Marken oder eingetragene Marken von BlackBerry Limited, deren Tochtergesellschaften und/oder angegliederten Unternehmen, die unter Lizenz verwendet werden. Das exklusive Recht an diesen Marken wird ausdrücklich vorbehalten. Alle weiteren Marken sind Eigentum ihrer jeweiligen Inhaber.

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

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

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

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



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

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

DIE IN DIESEM DOKUMENT GENANNTE EINSCHRÄNKUNGEN, AUSSCHLÜSSE UND HAFTUNGSAUSSCHLÜSSE GELTEN (A) UNGEACHTET DER VON IHNEN ANGEFÜHRTE 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 GRUNDLEGENDE ZWECK DIESER VEREINBARUNG ODER EINES DARIN ENTHALTENE RECHTSBEHELFS WIRKSAM; UND GELTEN (B) FÜR BLACKBERRY UND DIE ZUGEHÖRIGEN UNTERNEHMEN, RECHTSNACHFOLGER, BEVOLLMÄCHTIGTE, VERTRETER, LIEFERANTE (EINSCHLIESSLICH MOBILFUNKANBIETERN), AUTORISIERTE BLACKBERRY-DISTRIBUTOREN (EBENFALLS EINSCHLIESSLICH MOBILFUNKANBIETERN) UND DIE JEWEILIGEN FÜHRUNGSKRÄFTE, ANGESTELLTE UND UNABHÄNGIGE AUFTRAGNEHMER.

ZUSÄTZLICH ZU DEN OBEN GENANNTE EINSCHRÄNKUNGEN UND AUSSCHLÜSSEN HAFTEN DIE FÜHRUNGSKRÄFTE, ANGESTELLTE, VERTRETER, DISTRIBUTOREN, LIEFERANTE, UNABHÄNGIGE AUFTRAGNEHMER VON BLACKBERRY ODER BLACKBERRY ANGEHÖRENDE UNTERNEHMEN IN KEINER WEISE IM ZUSAMMENHANG MIT DER DOKUMENTATION.

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

Die Nutzungsbedingungen für BlackBerry-Produkte und -Dienste werden in einer entsprechenden separaten Lizenz oder anderen Vereinbarung mit BlackBerry dargelegt. KEINE PASSAGE IN DIESEM DOKUMENT IST DAZU VORGESEHEN, BELIEBIGE SCHRIFTLICHE VEREINBARUNGEN ODER GARANTIE, 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