BlackBerry UEM

Schützen von Netzwerkverbindungen

Verwalten

12.17

Inhalt

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

Verwalten von geschäftlichen Verbindungen mithilfe von Profilen

Mithilfe der folgenden Profile können Sie konfigurieren, wie Geräte eine Verbindung zu geschäftlichen Ressourcen 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	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.
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.
SSO-Erweiterung	Ein Profil für die SSO-Erweiterung legt fest, wie iOS- und iPadOS-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-Profile verwenden, um festzulegen, wie Geräte eine Verbindung zu geschäftlichen Wi-Fi-Netzwerken hinter der Firewall herstellen. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Wi-Fi-Profil zuweisen.

Standardmäßig können sowohl geschäftliche als auch persönliche Apps die auf dem Gerät gespeicherten Wi-Fi-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen.

Erstellen eines Wi-Fi-Profils

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

Bevor Sie beginnen:

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

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > WLAN**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Wi-Fi-Profil ein. Diese Informationen werden auf den Geräten angezeigt.
5. Geben Sie im Feld **SSID** den Netzwerknamen eines Wi-Fi-Netzwerks ein.
6. Wenn das Wi-Fi-Netzwerk die SSID nicht sendet, aktivieren Sie das Kontrollkästchen **Verborgenes Netzwerk**.
7. 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 Ihre Organisation 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
- iPadOS
- macOS
- Android
- Windows

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

Einstellungen für iOS gelten auch für iPadOS-Geräte.

Bei macOS gelten Profile entweder 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: • Benutzer • Gerät Diese Einstellung ist nur für macOS gültig.
Automatisch dem Netzwerk beitreten	Diese Einstellung gibt an, ob ein Gerät dem Wi-Fi-Netzwerk automatisch hinzugefügt werden kann.
MAC-Randomisierung deaktivieren	Diese Einstellung legt fest, ob Geräte ihre MAC-Adressen zufällig zuweisen können, wenn sie eine Verbindung zum Wi-Fi-Netzwerk herstellen. Diese Einstellung steht nur für Geräte mit iOS oder iPadOS iOS 14 und höher zur Verfügung.

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist.
Netzwerktyp	Diese Einstellung legt eine Konfiguration für das Wi-Fi-Netzwerk fest. Hotspot-Konfigurationen stehen nur für iOS-, iPadOS- und macOS-Geräte zur Verfügung. Wenn Sie eine der Hotspot-Optionen auswählen, verwenden Sie nicht dasselbe Wi-Fi-Profil, um Einstellungen für andere Gerätetypen zu konfigurieren. Mögliche Werte: • Standard • Legacy-Hotspot • Hotspot 2.0 Der Standardwert ist „Standard“.
Angezeigter Betreibername	Diese Einstellung legt den Anzeigenamen des Hotspot-Betreibers fest. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Domänenname	Diese Einstellung legt den Domänennamen des Hotspot-Betreibers fest. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist. Wenn Sie diese Einstellung verwenden, ist die Einstellung „SSID“ nicht erforderlich.
Unternehmensbezeichner der Roaming-Konsortien	Diese Einstellung legt die Organisationsbezeichner der Roaming-Konsortien und Dienstanbieter fest, auf die über den Hotspot zugegriffen werden kann. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
NAI-Bereichsnamen	Diese Einstellung legt die NAI-Bereichsnamen fest, die ein Gerät authentifizieren können. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
MCC/MNCs	Diese Einstellung legt die MCC/MNC-Kombinationen fest, die Mobilfunknetzbetreiber identifizieren. Jeder Wert muss genau sechs Ziffern umfassen. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.
Verbindungsaufbau zu Roaming-Partnernetzwerken zulassen	Diese Einstellung legt fest, ob ein Gerät eine Verbindung zu Roaming-Partnern für den Hotspot aufbauen kann. Diese Einstellung ist nur dann gültig, wenn der „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist.

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Wenn die Einstellung „Netzwerktyp“ auf „Hotspot 2.0“ gesetzt ist, ist diese Einstellung auf „WPA2-Enterprise“ gesetzt. Mögliche Werte: • Keine • WEP persönlich • WEP Unternehmen • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise • WPA3-Personal • WPA3-Enterprise Der Standardwert ist „Keine“.
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“, „WPA2-Personal“ oder „WPA3-Personal“ gesetzt ist.
Protokolle	
Authentifizierungsprotokoll	Diese Einstellung legt die EAP-Methoden fest, die das Wi-Fi-Netzwerk unterstützt. Sie können mehrere EAP-Methoden auswählen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist. Mögliche Auswahlen: • TLS • TTLS • LEAP • PEAP • EAP-FAST • EAP-SIM • EAP-AKA

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Interne Authentifizierung	Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist. Mögliche Werte: • Keine • PAP • CHAP • MS-CHAP • MS-CHAPv2 • EAP Der Standardwert ist „MS-CHAPv2“.
PAC verwenden	Diese Einstellung legt fest, ob die EAP-FAST-Methode geschützte Anmeldeinformationen (Protected Access Credential) verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist.
PAC bereitstellen	Diese Einstellung legt fest, ob die EAP-FAST-Methode die Bereitstellung von geschützten Anmeldeinformationen zulässt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt und die Einstellung „PAC verwenden“ ausgewählt ist.
PAC anonym bereitstellen	Diese Einstellung legt fest, ob die EAP-FAST-Methode die anonyme Bereitstellung von geschützten Anmeldeinformationen zulässt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „EAP-FAST“ gesetzt ist und die Einstellungen „PAC verwenden“ und „PAC bereitstellen“ ausgewählt sind.
Authentifizierung	
Externe Identität für TTLS, PEAP und EAP-FAST	Diese Einstellung legt die externe Identität für einen Benutzer fest, die als Klartext gesendet wird. Sie können einen anonymen Benutzernamen festlegen, um die echte Identität des Benutzers zu verbergen (beispielsweise „anonym“). Der verschlüsselte Tunnel wird verwendet, um den echten Benutzernamen zur Authentifizierung beim Wi-Fi-Netzwerk zu senden. Wenn die externe Identität den Bereichsnamen enthält, um die Anforderung weiterzuleiten, muss es sich dabei um den tatsächlichen Bereich des Benutzers handeln (beispielsweise „anonym@Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“, „PEAP“ oder „EAP-FAST“ gesetzt ist.

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Im Wi-Fi-Profil enthaltenes Kennwort verwenden	Diese Einstellung legt fest, ob das Wi-Fi-Profil das Kennwort für die Authentifizierung enthält. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, das ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Im Wi-Fi-Profil enthaltenes Kennwort verwenden“ ausgewählt wurde.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt fest, welche Art der Authentifizierung ein Gerät verwendet, um eine Verbindung zum Wi-Fi-Netzwerk aufzubauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist. Mögliche Werte: • Keine • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen Der Standardwert ist „Keine“.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für das mit dem Wi-Fi-Profil verknüpfte Client-Zertifikat fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“ gesetzt ist. Mögliche Werte: • Einzelne Referenz • Variable Einfügung Der Standardwert ist „Einzelne Referenz“.

iOS und macOS: Wi-Fi-Profileinstellung	Beschreibung
Profil für freigegebenes Zertifikat	Diese Einstellung legt das Profil für das freigegebene Zertifikat mit dem Clientzertifikat fest, das ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Name des Clientzertifikats	Diese Einstellung legt den Namen des Clientzertifikats fest, das ein Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „SCEP“ gesetzt ist.
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist.
Vertrauen	
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WEP Enterprise“, „WPA-Enterprise“, „WPA2-Enterprise“ oder „ WPA3-Enterprise“ gesetzt ist. Mögliche Werte: • Einzelne Referenz • Variable Einfügung Der Standardwert ist „Einzelne Referenz“.

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

Android: Wi-Fi-Profileinstellungen

Android: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, mit dem Android-Geräte die Verbindung zu einem Proxy-Server herstellen, wenn das Gerät mit dem Wi-Fi-Netzwerk verbunden ist. Auf Geräten mit Android 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.
BSSID	Diese Einstellung legt die MAC-Adresse eines drahtlosen Zugriffspunkts im Wi-Fi-Netzwerk fest.
Primärer DNS	Diese Einstellung legt den primären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung gilt nur für Geräte, die Samsung Knox verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.
Sekundärer DNS	Diese Einstellung legt den sekundären DNS-Server in Dezimalschreibweise mit Punkt fest (beispielsweise „192.0.2.0“). Diese Einstellung gilt nur für Geräte, die Samsung Knox verwenden, wenn die IP-Adresse über das Unternehmensnetzwerk statisch zugewiesen wird.
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Mögliche Werte: • Keine • Persönlich • Enterprise Der Standardwert ist „Keine“.
Persönlicher Sicherheitstyp	Diese Einstellung legt den persönlichen Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Persönlich“ gesetzt ist. Mögliche Werte: • Keine • WEP persönlich • WPA-Personal/WPA2-Personal Der Standardwert ist „Keine“.

Android: Wi-Fi-Profileinstellung	Beschreibung
WEP-Schlüssel	Diese Einstellung legt den WEP-Schlüssel für das Wi-Fi-Netzwerk fest. Der WEP-Schlüssel muss 10 oder 26 hexadezimale Zeichen (0-9, A-F) oder 5 bzw. 13 alphanumerische Zeichen (0-9, A-Z) umfassen. Beispiele für hexadezimale Schlüsselwerte sind „ABCDEF0123“ oder „ABCDEF0123456789ABCDEF0123“. Beispiele für alphanumerische Schlüsselwerte sind „abCD5“ oder „abCDefGHijKL1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WEP persönlich“ gesetzt ist.
Preshared key	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Persönlicher Sicherheitstyp“ auf „WPA-Personal/WPA2-Personal“ gesetzt ist.
Authentifizierungsprotokoll	Diese Einstellung legt die EAP-Methode fest, die das Wi-Fi-Netzwerk verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist. Mögliche Werte: • TLS • TTLS • PEAP • LEAP Der Standardwert ist „TLS“. LEAP wird von Geräten, die Samsung Knox verwenden, nicht unterstützt.
Interne Authentifizierung	Diese Einstellung legt fest, welche interne Authentifizierungsmethode mit TTLS verwendet wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungsprotokoll“ auf „TTLS“ gesetzt ist. Mögliche Werte: • Keine • PAP • CHAP • MS-CHAP • MS-CHAPv2 • GTC Der Standardwert ist „MS-CHAPv2“. CHAP wird von Geräten, die Samsung Knox verwenden, nicht unterstützt.

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

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

Android: Wi-Fi-Profileinstellung	Beschreibung
Verknüpftes Profil für Benutzeranmelde-informationen	Diese Einstellung legt das verknüpfte Profil für Benutzeranmeldeinformationen fest, das ein Android-Gerät verwendet, um ein Clientzertifikat für die Authentifizierung beim Wi-Fi-Netzwerk abzurufen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Benutzeranmeldeinformationen“ gesetzt ist. Der Name des Profils für Benutzeranmeldeinformationen muss für Geräte, die einen Knox Workspace verwenden, weniger als 36 Zeichen enthalten.
Name des Clientzertifikats	Diese Einstellung legt den Namen des Clientzertifikats fest, das ein Android-Gerät verwendet, um sich beim Wi-Fi-Netzwerk zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.
Vom Authentifizierungsserver erwartete allgemeine Zertifikatnamen	Diese Einstellung legt die allgemeinen Namen im Zertifikat fest, die der Authentifizierungsserver an das Gerät sendet (beispielsweise „*.Beispiel.com“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist.
Typ der Zertifikatverknüpfung	Diese Einstellung legt den Typ der Zertifikatverknüpfung für die mit dem Wi-Fi-Profil verknüpften vertrauenswürdigen Zertifikate fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „Unternehmen“ gesetzt ist. Mögliche Werte: • Einzelne Referenz • Variable Einfügung Der Standardwert ist „Einzelne Referenz“.
Zertifizierungsstellenzertifi Profil	Diese Einstellung legt das Profil mit Zertifizierungsstellenzertifikat mit dem vertrauenswürdigen Zertifikat fest, die ein Android-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Einzelne Referenz“ gesetzt ist.
Vertrauenswürdige Zertifikatnamen	Diese Einstellung legt die Namen der vertrauenswürdigen Zertifikate fest, die ein Android-Gerät verwendet, damit das Wi-Fi-Netzwerk als vertrauenswürdig gilt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Zertifikatverknüpfung“ auf „Variable Einfügung“ gesetzt ist.

Windows: Wi-Fi-Profileinstellungen

Windows: Wi-Fi-Profileinstellung	Beschreibung
Automatisch verbinden, wenn das Netzwerk in Reichweite ist	Diese Einstellung gibt an, ob Geräte automatisch eine Verbindung mit dem Wi-Fi-Netzwerk herstellen können.
Sicherheitstyp	Diese Einstellung legt den Sicherheitstyp fest, den das Wi-Fi-Netzwerk verwendet. Mögliche Werte: • Offen • WPA-Enterprise • WPA-Personal • WPA2-Enterprise • WPA2-Personal 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: • Keine • WEP • TKIP • AES
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	Diese Einstellung legt den vorinstallierten Schlüssel für das Wi-Fi-Netzwerk fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Personal“ gesetzt ist.
Single Sign-On aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die Authentifizierung nach einmaliger Anmeldung unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.
Typ der einmaligen Anmeldung	Diese Einstellung legt fest, wann die Authentifizierung nach einmaliger Anmeldung durchgeführt wird. Wenn diese Einstellung auf „Direkt vor Benutzeranmeldung durchführen“ gesetzt ist, wird die einmalige Anmeldung durchgeführt, bevor sich der Benutzer 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. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde. Mögliche Werte: • Direkt vor Benutzeranmeldung durchführen • Direkt nach Benutzeranmeldung durchführen Der Standardwert ist „Direkt vor Benutzeranmeldung durchführen“.
Maximale Verzögerung für Konnektivität	Diese Einstellung legt fest, wie viele Sekunden verstreichen sollen, bevor der Versuch, die Verbindung durch eine einmalige Anmeldung aufzubauen, fehlschlägt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde. Mögliche Werte sind 0 bis 120 Sekunden. Der Standardwert ist 10 Sekunden.
Zulassen, dass weitere Dialoge während der einmaligen Anmeldung angezeigt werden.	Diese Einstellung legt fest, ob ein Gerät außer dem Anmeldebildschirm Dialogfelder anzeigen kann. Wenn es beispielsweise für einen EAP-Authentifizierungstyp erforderlich ist, dass der Benutzer das im Authentifizierungsvorgang vom Server gesendete Zertifikat bestätigt, kann das Gerät das entsprechende Dialogfeld anzeigen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.

Windows: Wi-Fi-Profileinstellung	Beschreibung
Dieses Netzwerk verwendet separate virtuelle LANs für Geräte- und Benutzerauthentifizierung	Diese Einstellung legt fest, ob von den Anmeldeinformationen des Benutzers abhängt, welches VLAN von einem Gerät verwendet wird. Wenn das Gerät beispielsweise beim Starten in ein VLAN platziert wird und dann – basierend auf Berechtigungen – nach der Anmeldung des Benutzers in ein anderes VLAN-Netzwerk übergeht. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Single Sign-On aktivieren“ ausgewählt wurde.
Serverzertifikat bewerten	Diese Einstellung legt fest, ob ein Gerät das Serverzertifikat bewerten muss, das die Identität des drahtlosen Zugriffspunkts überprüft. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.
Benutzer nicht auffordern, neue Server oder vertrauenswürdige Zertifizierungsstellen zu autorisieren	Diese Einstellung legt fest, ob ein Benutzer aufgefordert wird, dem Serverzertifikat zu vertrauen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Serverzertifikat bewerten“ ausgewählt wurde.
Profile für Zertifizierungsstellenzertifi	Diese Einstellung legt das Profil des Zertifizierungsstellenzertifikats fest, das den Vertrauensstamm für das vom drahtlosen Zugriffspunkt verwendete Serverzertifikat bereitstellt. Diese Einstellung begrenzt die Stammzertifizierungsstellen, denen Geräte vertrauen, auf die ausgewählten Zertifizierungsstellen. Wenn Sie keine vertrauenswürdigen Stammzertifizierungsstellen auswählen, vertrauen die Geräte allen Stammzertifizierungsstellen, die in ihrem Speicher für vertrauenswürdige Stammzertifizierungsstellen aufgelistet sind. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Serverzertifikat bewerten“ ausgewählt wurde.
Schnelle Wiederherstellung der Verbindung aktivieren	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk die schnelle Wiederherstellung bei PEAP-Authentifizierung über mehrere drahtlose Zugriffspunkte unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.
NAP erzwingen	Diese Einstellung legt fest, ob das Wi-Fi-Netzwerk anhand von NAP Systemintegritätsprüfungen auf Geräten durchführen soll, um zu überprüfen, ob die Geräte den Integritätsanforderungen entsprechen, bevor der Verbindungsaufbau zum Netzwerk zugelassen wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA-Enterprise“ oder „WPA2-Enterprise“ gesetzt ist.

Windows: Wi-Fi-Profileinstellung	Beschreibung
FIPS-Modus aktivieren	Diese Einstellung gibt an, ob das Wi-Fi-Netzwerk mit dem FIPS 140-2-Standard konform ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA2-Enterprise“ oder „WPA2-Personal“ und der „Verschlüsselungstyp“ auf „WEP“ festgelegt sind.
PMK-Zwischenspeicherung aktivieren	Diese Einstellung legt fest, ob ein Gerät den PMK zwischenspeichern kann, um ein schnelles WPA2 Roaming einzuschalten. Ein schnelles Roaming überspringt 802.1X-Einstellungen mit einem drahtlosen Zugriffspunkt, bei dem sich das Gerät zuvor authentifiziert hat. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Sicherheitstyp“ auf „WPA2-Enterprise“ gesetzt ist.
PMK-Lebenszeit	Diese Einstellung legt fest, wie viele Minuten ein Gerät den PMK im Cache speichern kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde. Mögliche Werte sind 5 bis 1440 Minuten. Der Standardwert ist 720 Minuten.
Anzahl der Einträge im PMK-Cache	Diese Einstellung legt die maximale Anzahl an PMK-Einträgen fest, die ein Gerät im Cache speichern kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde. Mögliche Werte sind 1 bis 255. Der Standardwert ist 128.
Dieses Netzwerk arbeitet mit Vorauthentifizierung	Diese Einstellung legt fest, ob der Zugriffspunkt die Vorauthentifizierung für ein schnelles WPA2 Roaming unterstützt. Vorauthentifizierung ermöglicht Geräten, die eine Verbindung zu einem drahtlosen Zugriffspunkt aufbauen, 802.1X-Einstellungen mit anderen drahtlosen Zugriffspunkten innerhalb seines Bereichs durchzuführen. Bei einer Vorauthentifizierung werden der PMK und die mit ihm verknüpften Informationen im PMK-Cache gespeichert. Wenn das Gerät eine Verbindung zu einem drahtlosen Zugriffspunkt aufbaut, bei dem es sich vorauthentifiziert hat, verwendet es die zwischengespeicherten PMK-Daten, um die Zeit für die Authentifizierung und den Verbindungsaufbau zu verkürzen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „PMK-Zwischenspeicherung aktivieren“ ausgewählt wurde.

Windows: Wi-Fi-Profileinstellung	Beschreibung
Maximale Anzahl der Vorauthentifizierungsversu	Diese Einstellung legt die maximale Anzahl zulässiger Vorauthentifizierungsversuche fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Dieses Netzwerk arbeitet mit Vorauthentifizierung“ ausgewählt wurde. Mögliche Werte sind 1 bis 16. Der Standardwert ist 3.
Proxy-Typ	Diese Einstellung legt den Typ der Proxy-Konfiguration für das Wi-Fi-Profil fest. Mögliche Einstellungen: • Keine • PAC-Konfiguration • Manuelle Konfiguration • Web-Proxy automatisch erkennen Die Standardeinstellung ist „Manuelle Konfiguration“. Diese Einstellung gilt nur für Windows 10 Mobile-Geräte.
PAC-URL	Diese Einstellung gibt die URL für den Webserver an, der die PAC-Datei hostet, einschließlich PAC-Dateinamen im Format http://<web_server_URL>/<filename>.pac. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „PAC-Konfiguration“ gesetzt ist.
Adresse	Diese Einstellung gibt den Servernamen und Port für den Netzwerk-Proxy an. Verwenden Sie das Format „Host:Port“ (z. B. server01.beispiel.com:123). Der Host muss einer der folgenden sein: • Ein registrierter Name, z. B ein Servername, FQDN oder ein einzelner Etikettenname (z. B. "server01" anstatt server01.beispiel.com) • Eine IPv4- oder IPv6-Adresse Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Manuelle Konfiguration“ gesetzt ist.
Web-Proxy automatisch erkennen	Diese Einstellung gibt an, ob das WPAD-Protokoll (Web Proxy Autodiscovery Protocol) für die Proxy-Suche aktiviert werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Web-Proxy automatisch erkennen“ gesetzt ist. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Überprüfung der Internetverbindung deaktivieren	Diese Einstellung legt fest, ob Überprüfungen der Internetverbindung deaktiviert werden sollen. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

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.

Einrichten von geschäftlichen VPNs für Geräte

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

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

Gerät	App- und Netzwerkverbindungen
iOS und iPadOS	Geschäftliche und private Apps können die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Sie können Per App VPN für ein VPN-Profil aktivieren, um das Profil nur auf die festgelegten geschäftlichen Apps anzuwenden. Sie können VPN bei Bedarf aktivieren, damit Geräte automatisch eine Verbindung zu einem VPN in einer bestimmten Domäne herstellen. Sie können z. B. die Domäne Ihres Unternehmens angeben, um Benutzern den Zugriff auf den Inhalt Ihres Intranets mithilfe von VPN bei Bedarf zu gestatten.
macOS	Konfigurieren Sie VPN-Profile, um das Herstellen einer Verbindung zu Ihrem Unternehmensnetzwerk über Apps zu ermöglichen. Sie können VPN bei Bedarf aktivieren, damit Geräte automatisch eine Verbindung zu einem VPN in einer bestimmten Domäne herstellen. Sie können z. B. die Domäne Ihres Unternehmens angeben, um Benutzern den Zugriff auf den Inhalt Ihres Intranets mithilfe von VPN bei Bedarf zu gestatten.
Samsung Knox	Auf Samsung Knox-Geräten, die über Android Enterprise- oder Samsung Knox Workspace-Aktivierungen verfügen, können geschäftliche Apps die auf dem Gerät gespeicherten VPN-Profile verwenden, um eine Verbindung zum Netzwerk Ihrer Organisation herzustellen. Sie können Per App VPN aktivieren, um das Profil nur auf die festgelegten geschäftlichen Apps anzuwenden. Auf dem Gerät muss eine unterstützte VPN-Client-App installiert sein. Cisco AnyConnect und Juniper werden unterstützt. **Hinweis:** Die Juniper-App unterstützt nur SSL VPN.
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-Profils

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

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-, iPadOS-, macOS- und Samsung Knox-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**.

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

CylanceGATEWAY ist eine Cloud-native Lösung, die Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA) gestützt auf künstliche Intelligenz (KI) bietet. Wenn CylanceGATEWAY auf einem Gerät aktiviert ist, erstellen Sie ein ZTNA-Profil, das das Gerät als VPN-Anbieter erkennt. CylanceGATEWAY vertraut standardmäßig nichts und niemandem.

- CylanceGATEWAY schützt die iOS-, Android-, Windows 10-, Windows 11- und macOS-Geräte der Benutzer, indem Sie Verbindungen zu Internetzielen blockieren können, mit denen die Geräte nicht kommunizieren sollen, selbst wenn das Gerät nicht mit Ihrem Netzwerk verbunden ist.
- Zusätzlich zum Schutz von Geräten schützt CylanceGATEWAY den Zugriff auf das private Netzwerk und die Cloud-basierten Anwendungen Ihres Unternehmens, indem kontinuierlich analysiert wird, ob es sich um erwartetes Nutzungsverhalten der Benutzer oder um ungewöhnliches Verhalten handelt. Wenn der Prozentsatz der anormalen Ereignisse einen festgelegten Schwellenwert überschreitet, kann CylanceGATEWAY die Netzwerkzugriffssteuerungsrichtlinie des Benutzers dynamisch außer Kraft setzen, um den Netzwerkzugriff zu blockieren und den Benutzer zur Authentifizierung aufzufordern, bevor er fortfahren kann.

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

Weitere Informationen zur Einrichtung von CylanceGATEWAY finden Sie unter Einrichten von BlackBerry Gateway in der Dokumentation zur Cylance Endpoint Security-Einrichtung.

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
- iPadOS
- macOS
- Samsung Knox
- Windows 10

iOS und macOS: VPN-Profileinstellungen

Einstellungen für iOS gelten auch für iPadOS-Geräte.

Bei macOS gelten Profile entweder 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	Diese Einstellung gibt an, ob das VPN-Profil auf einem macOS-Gerät für das Benutzerkonto oder das Gerät gilt. Mögliche Werte: • Benutzer • Gerät Diese Einstellung ist nur für macOS-Geräte gültig.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Verbindungstyp	Diese Einstellung legt den Verbindungstyp fest, den ein Gerät für ein VPN-Gateway verwendet. Bei einigen Verbindungstypen müssen die Benutzer außerdem die entsprechende VPN-App auf dem Gerät installieren. Mögliche Werte: • L2TP • PPTP • IPSec • Cisco AnyConnect • Juniper • Pulse Secure • F5 • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile • OpenVPN • Benutzerdefiniert • IKEv2 • IKEv2 Immer An Der Standardwert ist „L2TP“. Wenn Sie „IKEv2 Immer An“ wählen, gelten für viele Einstellungen separate Werte für Mobilfunk- und Wi-Fi-Verbindungen. Einige Werte sind für macOS-Geräte nicht gültig.
VPN-Bundle-ID	Diese Einstellung legt die Bundle-ID der VPN-App für ein benutzerdefiniertes SSL-VPN fest. Die Bundle-ID wird im umgekehrten DNS-Format angegeben (beispielsweise „com.example.VPNapp“). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.
Server	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable angeben.
Benutzerdefinierte Schlüsselwertepaare	Diese Einstellung legt die Schlüssel und die verknüpften Werte für das benutzerdefinierte SSL-VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Benutzerdefiniert“ gesetzt ist.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Anmeldegruppe oder Domäne	Diese Einstellung legt die Anmeldegruppe oder -domäne fest, die das VPN-Gateway verwendet, um ein Gerät zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SonicWALL Mobile Connect“ gesetzt ist.
Bereich	Diese Einstellung legt den Namen des Authentifizierungsbereichs fest, den das VPN-Gateway verwendet, um ein Gerät zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ oder „Pulse Secure“ gesetzt ist.
Rolle	Diese Einstellung legt den Namen der Benutzerrolle fest, den ein VPN-Gateway verwendet, um die Netzwerkressourcen zu überprüfen, auf die ein Gerät zugreifen kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Juniper“ oder „Pulse Secure“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest. Die Einstellung „Verbindungstyp“ legt fest, welche Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • Kennwort • RSA SecurID • Gemeinsamer geheimer Schlüssel • Gemeinsamer geheimer Schlüssel/Gruppenname • Freigegebenes Zertifikat • SCEP • Benutzeranmeldeinformationen
EAP-Plug-Ins	Diese Einstellung legt die Authentifizierungs-Plug-Ins für das VPN fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ oder „PPTP“ und die Einstellung „Authentifizierungstyp“ auf „RSA SecurID“ gesetzt ist.
Authentifizierungsprotokoll	Diese Einstellung legt die Authentifizierungsprotokolle für das VPN fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „L2TP“ oder „PPTP“ und die Einstellung „Authentifizierungstyp“ auf „RSA SecurID“ gesetzt ist.
Kennwort	Diese Einstellung legt das Kennwort fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierungstyp“ auf „Kennwort“ gesetzt ist.

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

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

iOS und macOS: VPN-Profileinstellung	Beschreibung
Remote-ID	Diese Einstellung legt die Remote-ID des IKEv2-Clients in einem der folgenden Formate fest: FQDN, Benutzer-FQND, Adresse oder ASN1DN. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
VPN bei Bedarf aktivieren	Diese Einstellung legt fest, ob ein Gerät automatisch beim Zugriff auf bestimmte Domänen eine VPN-Verbindung herstellen kann. Diese Einstellung betrifft geschäftliche Apps auf iOS- und iPadOS-Geräten. Diese Einstellung gilt nur unter den folgenden Bedingungen: • Die Einstellung „Verbindungstyp“ ist auf „IPsec“, „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ und der „Authentifizierungstyp“ auf „Freigegebenes Zertifikat“, „SCEP“ oder „Benutzeranmeldeinformationen“ gesetzt. • Die Einstellung „Anschlusstyp“ ist auf „IKEv2“ und der „Authentifizierungstyp“ auf „Gemeinsames Zertifikat“ gesetzt.
Domänen- oder Hostnamen, die "VPN auf Abruf" verwenden können	Diese Einstellung legt die Domänen und die verknüpften Aktionen für VPN bei Bedarf fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist. Mögliche Werte für die „Bei Bedarf-Aktion“: • Immer herstellen • Herstellen, wenn erforderlich • Niemals herstellen
Regeln für „VPN bei Bedarf“ für iOS 7.0 und höher	Diese Einstellung legt die Verbindungsanforderungen für VPN bei Bedarf fest. Sie müssen einen oder mehrere Schlüssel aus dem Beispiel für das Nutzlastformat verwenden. Diese Einstellung überschreibt die Einstellung „Domänen- oder Hostnamen, die VPN bei Bedarf verwenden können“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.
Verbindung bei Leerlauf trennen	Diese Einstellung legt fest, ob die VPN-Verbindung getrennt wird, wenn sie für einen bestimmten Zeitraum inaktiv ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN bei Bedarf aktivieren“ ausgewählt ist.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Verbindung gemäß Leerlauf-Timer trennen	Diese Einstellung gibt die Leerlaufzeit in Sekunden an, nach der die VPN-Verbindung getrennt wird. Der Standardwert ist „120“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindung bei Leerlauf trennen“ ausgewählt wurde.
Benutzer dürfen VPN nicht bei Bedarf deaktivieren	Diese Einstellung legt fest, ob der Benutzer das VPN bei Bedarf deaktivieren kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“, „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 14 und höher.
Lokales Netzwerk ausschließen	Diese Einstellung legt fest, ob lokaler Netzwerkdatenverkehr von der Verwendung der VPN-Verbindung ausgenommen wird. Wenn die Einstellung „Alle Netzwerke einschließen“ ebenfalls ausgewählt ist, wird kein lokaler Netzwerkdatenverkehr über das VPN weitergeleitet. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13 und höher.
Alle nicht standardmäßigen Weiterleitungen haben Vorrang vor allen lokal definierten Weiterleitungen	Diese Einstellung legt fest, ob die nicht standardmäßigen Weiterleitungen für das VPN Vorrang vor lokal definierten Weiterleitungen haben. Wenn die Einstellung „Alle Netzwerke einschließen“ ebenfalls ausgewählt ist, wird diese Einstellung ignoriert. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 14,2 und höher.
Alle Netzwerke einschließen	Diese Einstellung legt fest, ob der gesamte Netzwerkverkehr über das VPN weitergeleitet werden soll. Wenn auch „Lokales Netzwerk ausschließen“ ausgewählt ist, wird der lokale Netzwerkverkehr nicht über das VPN geleitet. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13 und höher.
Festgelegter Anbieter	Diese Einstellung gibt einen festgelegten VPN-Anbieter an. Wenn der VPN-Anbieter als Systemerweiterung implementiert ist, ist diese Einstellung erforderlich. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IPsec“, „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“ oder „Benutzerdefiniert“ gesetzt ist.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Deaktivierung der automatischen Verbindung durch Benutzer zulassen	Diese Einstellung legt fest, ob Benutzer die VPN-Verbindung deaktivieren können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist.
Gleiche Tunnelkonfiguration für Mobilfunk und Wi-Fi verwenden	Diese Einstellung legt fest, ob Sie separate VPN-Einstellungen für das Gerät festlegen möchten, je nachdem, ob das Gerät Daten über ein Mobilfunknetz oder ein Wi-Fi-Netzwerk sendet. Wenn diese Einstellung nicht ausgewählt ist, können Sie unterschiedliche Mobilfunk- und Wi-Fi-Einstellungen im selben Profil festlegen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist.
xAuth aktivieren	Diese Einstellung legt fest, ob das VPN die erweiterte Authentifizierung (xAuth) unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
TLS-Mindestversion	Diese Einstellung gibt die minimale TLS-Version an, die Geräte für die EAP-TLS-Authentifizierung verwenden. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist. Mögliche Werte: • 1.0 • 1.1 • 1.2 Die Standardeinstellung ist „1.0“.
Höchste unterstützte TLS-Version	Diese Einstellung gibt die höchste unterstützte TLS-Version an, die Geräte für die EAP-TLS-Authentifizierung verwenden. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist. Mögliche Werte: • 1.0 • 1.1 • 1.2 Die Standardeinstellung ist „1.2“.
Zertifikattyp	Diese Einstellung gibt den Zertifikattyp an, der für die IKEv2-Computerauthentifizierung verwendet wird. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Allgemeiner Name des Serverzertifikatausstellers	Diese Einstellung gibt den allgemeinen Namen der Zertifizierungsstelle an, die das Zertifikat ausgestellt hat, das der IKE-Server an das Gerät sendet. Wenn Sie xAuth mithilfe eines Zertifikats aktivieren, ist diese Einstellung erforderlich. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.
Allgemeiner Name des Serverzertifikats	Diese Einstellung gibt den allgemeinen Namen des Serverzertifikats an, das der IKE-Server an das Gerät sendet. Diese Einstellung ist nur gültig, wenn die Einstellung „xAuth aktivieren“ ausgewählt und der Authentifizierungstyp auf „Zertifikat“ gesetzt ist.
Keep-alive-Intervall	Diese Einstellung legt fest, wie häufig ein Gerät ein Keep-alive-Paket sendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist. Mögliche Werte: • Deaktiviert • 30 Minuten • 10 Minuten • 1 Minute Die Standardeinstellung ist „10 Minuten“.
MOBIKE deaktivieren	Diese Einstellung legt fest, ob MOBIKE deaktiviert ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
IKEv2-Umleitung deaktivieren	Diese Einstellung legt fest, ob die IKEv2-Umleitung deaktiviert ist. Wenn diese Einstellung nicht aktiviert ist, wird die IKEv2-Verbindung umgeleitet, wenn eine Umleitungsanfrage vom Server empfangen wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Perfekte Geheimhaltung bei der Weiterleitung aktivieren	Diese Einstellung legt fest, ob das VPN PFS unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
NAT-Keep-alive aktivieren	Diese Einstellung legt fest, ob das VPN NAT-Keep-alive-Pakete unterstützt. Keep-alive-Pakete werden zur Aufrechterhaltung der NAT-Zuordnungen für IKEv2-Verbindungen verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.

iOS und macOS: VPN-Profileinstellung	Beschreibung
NAT-Keep-alive-Intervall	Diese Einstellung legt fest, wie häufig ein Gerät ein NAT-Keep-alive-Paket sendet (in Sekunden). Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt und die Einstellung „NAT-Keep-alive aktivieren“ ausgewählt ist. Der Mindest- und der Standardwert ist 20.
Interne IPv4- und IPv6-IKEv2-Subnetze verwenden	Diese Einstellung legt fest, ob das VPN die Attribute INTERNAL_IP4_SUBNET und INTERNAL_IP6_SUBNET der IKEv2-Konfiguration verwenden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Allgemeiner Name des Serverzertifikats	Diese Einstellung gibt den allgemeinen Namen in dem Zertifikat an, das der IKE-Server an das Gerät sendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Allgemeiner Name des Serverzertifikatausstellers	Diese Einstellung gibt den allgemeinen Namen des Zertifikatsausstellers in dem Zertifikat an, das der IKE-Server an das Gerät sendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Zertifikatswiderrufprüfung aktivieren	Diese Einstellung gibt an, ob der Versuch einer Zertifikatswiderrufprüfung für das Serverzertifikat erfolgt. Die Prüfung schlägt nicht fehl, wenn keine Reaktion erfolgt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Fallback aktivieren	Diese Einstellung legt fest, ob das Gerät einen VPN-Tunnel über das Mobilfunknetz einrichten kann, wenn Wi-Fi Assist aktiviert ist. Diese Einstellung gilt nur für Geräte mit iOS und iPadOS 13 oder höher und erfordert, dass der Server mehrere Tunnel für einzelne Benutzer unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Untergeordnete Sicherheitszuordnungsparar anwenden	Diese Einstellung gibt an, ob untergeordnete Sicherheitszuordnungsparameter angewendet werden sollen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
IKE-Sicherheitszuordnungsparameter anwenden	Diese Einstellung gibt an, ob IKE-Sicherheitszuordnungsparameter angewendet werden sollen. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.

iOS und macOS: VPN-Profileinstellung	Beschreibung
MTU	Diese Einstellung gibt die maximale Übertragungseinheit in Byte an. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 14 und höher. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist.
Mailbox	Diese Einstellung legt fest, ob Verbindungen zum Mailbox-Dienst über den VPN-Tunnel gesendet, außerhalb des VPN-Tunnels gesendet oder blockiert werden. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13,4 und höher. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Sie gilt nur für Wi-Fi-Verbindungen.
AirPrint	Diese Einstellung legt fest, ob AirPrint AirPrint-Verbindungen über den VPN-Tunnel gesendet, außerhalb des VPN-Tunnels gesendet oder blockiert werden. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13,4 und höher. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Sie gilt nur für Wi-Fi-Verbindungen.
Datenverkehr von Captive-Websheet außerhalb des VPN-Tunnels zulassen	Diese Einstellung legt fest, ob Datenverkehr von Captive Websheets außerhalb des VPN-Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Sie gilt nur für Wi-Fi-Verbindungen.
Datenverkehr sämtlicher Captive-Netzwerk-Apps außerhalb des VPN-Tunnels zulassen	Diese Einstellung legt fest, ob Datenverkehr von allen Captive-Netzwerk-Apps außerhalb des VPN-Tunnels gesendet werden kann. Wenn diese Einstellung nicht aktiviert ist, können Sie einzelne Apps angeben, für die Datenverkehr außerhalb des Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Sie gilt nur für Wi-Fi-Verbindungen.
Datenverkehr dieser Apps ist außerhalb des VPN-Tunnels zulässig	Diese Einstellung legt einzelne Captive-Netzwerk-Apps fest, für die Datenverkehr außerhalb des Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Sie gilt nur für Wi-Fi-Verbindungen.
App-Datenverkehr außerhalb des VPN-Tunnels zulassen	Diese Einstellung legt Apps fest, deren Datenverkehr außerhalb des Tunnels gesendet werden kann. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „IKEv2 Immer An“ gesetzt ist. Sie gilt nur für Wi-Fi-Verbindungen.

iOS und macOS: VPN-Profileinstellung	Beschreibung
DH-Gruppe	Diese Einstellung gibt die DH-Gruppe an, die ein Gerät zur Generierung des Schlüssels verwendet. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist. Mögliche Werte: • 0 • 1 • 2 • 5 • 14 • 15 • 16 • 17 • 18 • 19 • 20 • 21 • 31 Die Standardeinstellung ist „2“.
Verschlüsselungsalgorithmu	Diese Einstellung legt den IKE-Verschlüsselungsalgorithmus fest. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist. Mögliche Werte: • DES • 3DES • AES 128 • AES 256 • AES 128 GCM • AES 256 GCM • ChaCha20Poly1305 Die Standardeinstellung ist „3DES“.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Integritätsalgorithmus	Diese Einstellung legt den IKE-Integritätsalgorithmus fest. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist. Mögliche Werte: • SHA1 96 • SHA1 160 • SHA1 256 • SHA2 384 • SHA2 512 Der Standardwert ist „SHA1-96“.
Schlüsseländerungsintervall	Diese Einstellung legt die Lebensdauer der IKE-Verbindung fest. Diese Einstellung ist nur gültig, wenn die Einstellung „Untergeordnete Sicherheitszuordnungsparameter anwenden“ oder „IKE-Sicherheitszuordnungsparameter anwenden“ ausgewählt ist. Mögliche Werte sind 10 bis 1440 Minuten. Der Standardwert ist 1440.
Per App VPN aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway Per App VPN unterstützt. Mit dieser Funktion kann die Belastung im VPN einer Organisation reduziert werden. So könnten Sie beispielsweise festlegen, dass nur ein bestimmter geschäftlicher Datenverkehr, wie etwa der Zugriff auf Anwendungsserver oder Webseiten, über das VPN abgewickelt wird. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Cisco AnyConnect“, „Juniper“, „Pulse Secure“, „F5“, „SonicWALL Mobile Connect“, „Aruba VIA“, „Check Point Mobile“, „OpenVPN“, „Benutzerdefiniert“, „IKEv2“ oder „IKEv2 Immer An“ gesetzt ist.
Zulassen, dass Apps automatisch eine Verbindung herstellen	Diese Einstellung legt fest, ob mit Per App VPN verknüpfte Apps die VPN-Verbindung automatisch starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.
Safari-Domänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung in Safari starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist.

iOS und macOS: VPN-Profileinstellung	Beschreibung
Kalenderdomänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung im Kalender starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13.0 und höher.
Kontaktdomänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung in Kontakten starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13.0 und höher.
E-Mail-Domänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung im E-Mail-Programm starten können. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13.0 und höher.
Zugeordnete Domänen	Diese Einstellung legt die Domänen fest, die die VPN-Verbindung auf dem Gerät starten können. Die Domänen müssen auch in der Datei „apple-app-site-association“ enthalten sein. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 14.0 und höher.
Ausgeschlossene Domänen	Diese Einstellung gibt Domänen an, die am Starten der VPN-Verbindung auf dem Gerät gehindert werden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 14.0 und höher.
Datenverkehrs-Tunneling	Diese Einstellung legt fest, ob das VPN den Verkehr in der Anwendungsschicht oder IP-Schicht tunnelt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Per App VPN aktivieren“ ausgewählt ist. Diese Einstellung gilt nur für Geräte mit iOS oder iPadOS 13.0 und höher. Mögliche Werte: • Anwendungsschicht • IP-Schicht Die Standardeinstellung ist „Anwendungsschicht“.
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.

Android: VPN-Profileinstellungen

Die folgenden VPN-Profile werden nur auf Samsung Knox 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.

Android: VPN-Profileinstellung	Beschreibung
Serveradresse	Diese Einstellung legt den FQDN oder die IP-Adresse eines VPN-Servers fest.
VPN-Typ	Diese Einstellung legt fest, ob ein Gerät IPsec oder SSL verwendet, um eine Verbindung mit dem Mailserver aufzubauen. Mögliche Werte: • IPSec • SSL Der Standardwert ist „IPsec“. Die Juniper-VPN-App unterstützt nur SSL.
Benutzerauthentifizierung erforderlich	Diese Einstellung legt fest, ob ein Gerät einen Benutzernamen und ein Kennwort zum Herstellen einer Verbindung mit dem VPN-Server bereitstellen muss.
Benutzername	Diese Einstellung legt den Benutzernamen fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Wenn das Profil für mehrere Benutzer gilt, können Sie die %UserName%-Variable verwenden. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.
Kennwort	Diese Einstellung legt das Kennwort fest, den ein Gerät verwendet, um sich beim VPN-Gateway zu authentifizieren. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Benutzerauthentifizierung erforderlich“ ausgewählt wurde.
Split-Tunnel-Typ	Diese Einstellung legt fest, ob ein Gerät Split-Tunneling verwenden kann, um das VPN-Gateway zu umgehen, sofern dies vom VPN-Gateway unterstützt wird. Mögliche Werte: • Deaktiviert • Manuell • Automatisch Wenn der VPN-Typ auf „IPsec“ festgelegt ist, muss diese Einstellung auf „Deaktiviert“ festgelegt werden. Der Standardwert ist „Deaktiviert“.
Weiterleitungsrouten	Diese Einstellung legt die Route(n) zum Umgehen des VPN-Gateways fest. Sie können eine oder mehrere IP-Adressen angeben. Diese Einstellung ist nur dann gültig, wenn „VPN-Typ“ auf „SSL“ und der „Split-Tunnel-Typ“ auf „Manuell“ gesetzt ist.

Android: VPN-Profileinstellung	Beschreibung
DPD	Diese Einstellung legt fest, ob DPD aktiviert ist. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Version	Diese Einstellung gibt die Version des IKE-Protokolls zur Verwendung mit der VPN-Verbindung an. Mögliche Werte: • IKEv1 • IKEv2 Der Standardwert ist „IKEv1“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für die IPsec-VPN-Verbindung fest. Die Einstellung „IKE-Version“ legt fest, welche IPsec-Authentifizierungstypen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • Zertifikat • Preshared key • EAP MD5 • EAP MSCHAPv2 • Hybrid RSA • CAC-basierte Authentifizierung Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
ID-Typ der IPsec-Gruppe	Diese Einstellung legt den IPsec-Gruppen-ID-Typ für die VPN-Verbindung fest. Die Einstellung „IPsec-Authentifizierungstyp“ legt fest, welche IPsec-Gruppen-ID-Typen unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird. Mögliche Werte: • Standard • IPv4-Adresse • Fully Qualified Domain Name (vollständiger Domänenname) • Benutzer-FQDN • IKE-Schlüssel-ID Wird für „IPsec-Authentifizierungstyp“ die Einstellung „Zertifikat“ verwendet, dann wird diese Einstellung automatisch auf „Standard“ festgelegt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.

Android: VPN-Profileinstellung	Beschreibung
IPsec-Gruppen-ID	Diese Einstellung legt die IPsec-Gruppen-ID für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
Schlüsselaustauschmodus IKE-Phase-1	Diese Einstellung legt den Austauschmodus für die VPN-Verbindung fest. Mögliche Werte: • Hauptmodus • Aggressive-Modus Der Standardwert ist „Hauptmodus“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Lebensdauer	Diese Einstellung legt die Lebensdauer der IKE-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Verschlüsselungsalgorithmus	Diese Einstellung gibt den für eine IKE-Verbindung verwendeten Verschlüsselungsalgorithmus an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IKE-Integritätsalgorithmus	Diese Einstellung gibt den für eine IKE-Verbindung verwendeten Integritätsalgorithmus an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ und die „IKE-Version“ auf „IKEv2“ gesetzt ist.
IPsec DH-Gruppe	Diese Einstellung gibt die DH-Gruppe an, die ein Gerät zur Generierung des Schlüssels verwendet. Mögliche Werte sind 0, 1, 2, 5 und 14 bis 26. Der Standardwert ist 0. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Parameter	Diese Einstellung legt die IPsec-Parameter für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
Perfekte Geheimhaltung bei der Weiterleitung	Diese Einstellung legt fest, ob das VPN-Gateway PFS unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.

Android: VPN-Profileinstellung	Beschreibung
MOBIKE aktivieren	Diese Einstellung legt fest, ob das VPN-Gateway MOBIKE unterstützt. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Lebensdauer	Diese Einstellung legt die Lebensdauer der IPsec-Verbindung in Sekunden fest. Wenn Sie einen nicht unterstützten Wert oder einen Nullwert setzen, wird der Standardwert des Geräts verwendet. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Verschlüsselungsalgorithmu	Diese Einstellung legt den IPsec-Verschlüsselungsalgorithmus für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ gesetzt ist.
IPsec-Integritätsalgorithmus	Diese Einstellung legt den IPsec-Integritätsalgorithmus für die VPN-Verbindung fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „VPN-Typ“ auf „IPsec“ und die „IKE-Version“ auf „IKEv2“ gesetzt ist.
Authentifizierungstyp	Diese Einstellung legt den Authentifizierungstyp für das VPN-Gateway fest. Mögliche Werte: • Keine • Zertifikatsbasierte Authentifizierung • CAC-basierte Authentifizierung Der Standardwert ist „Keine“. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.
SSL-Algorithmus	Diese Einstellung gibt den für eine SSL-VPN-Verbindung erforderlichen Verschlüsselungsalgorithmus an. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „SSL“ gesetzt ist.
UID-/PID-Informationen anhängen	Diese Einstellung gibt an, ob UID/PID-Informationen an Pakete angehängt werden, die an den VPN-Client gesendet werden. Diese Einstellung muss für die Cisco AnyConnect VPN-App aktiviert werden.

Android: VPN-Profileinstellung	Beschreibung
Verkettung unterstützen	Diese Einstellung legt fest, wie die VPN-Verkettung unterstützt wird. Mögliche Werte: • Verkettung unterstützen • Äußerer Tunnel • Innerer Tunnel Der Standardwert ist „Verkettung unterstützen“.
Typ der Anbieterzeichenfolge	Diese Einstellung legt die Schlüsselwertpaare oder die JSON-Zeichenfolge für das VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters. Mögliche Werte: • Schlüsselwertpaare des Anbieters • JSON-Wert des Anbieters Der Standardwert lautet „Schlüsselwertpaare des Anbieters“.
Schlüsselwertpaare des Anbieters	Diese Einstellung legt die Schlüssel und die verknüpften Werte für das VPN fest. Die Konfigurationsinformationen sind spezifisch für die VPN-App des Anbieters. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Anbieterzeichenfolge“ auf „Schlüsselwertpaare des Anbieters“ gesetzt ist.
JSON-Wert des Anbieters	Diese Einstellung legt die Konfigurationsdaten für die VPN-App des Anbieters im .json-Format fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Typ der Anbieterzeichenfolge“ auf „JSON-Wert des Anbieters“ gesetzt ist.
Paket-ID des VPN-Clients	Diese Einstellung legt die Paket-ID der VPN-App fest.
Verbindung nach Fehler automatisch wiederherstellen	Diese Einstellung legt fest, ob die VPN-Verbindung nach Verbindungsverlust automatisch neu hergestellt werden soll.
FIPS-Modus aktivieren	Diese Einstellung legt fest, ob FIPS aktiviert ist. Durch Aktivieren des FIPS-Modus wird sichergestellt, dass nur FIPS-geprüfte Kryptografiealgorithmen für die VPN-Verbindung verwendet werden.
Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich	Diese Einstellung gibt an, ob Samsung Knox Workspace-Geräte eine VPN-Verbindung für alle Apps im geschäftlichen Bereich oder nur für bestimmte Apps verwenden. • „Containerweites VPN“ verwendet eine VPN-Verbindung für alle Apps im geschäftlichen Bereich auf dem Gerät. • „Per App VPN“ verwendet nur für die angegebenen Apps eine VPN-Verbindung.

Android: VPN-Profileinstellung	Beschreibung
Apps, die VPN-Verbindung verwenden dürfen	Diese Einstellung gibt die Apps im geschäftlichen Bereich an, die eine VPN-Verbindung verwenden können. Sie können Apps aus einer Liste verfügbarer Apps auswählen oder die App-Paket-ID angeben. Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Per App VPN“ gesetzt ist.
Verknüpftes Proxy-Profil	Diese Einstellung legt das verknüpfte Proxy-Profil fest, das ein Gerät verwendet, um eine Verbindung zu einem Proxy-Server aufzubauen, wenn das Gerät mit dem VPN verbunden ist.

Windows 10: VPN-Profileinstellungen

Windows: VPN-Profileinstellung	Beschreibung
Verbindungstyp	Diese Einstellung legt den Verbindungstyp fest, den ein Windows 10-Gerät für ein VPN verwendet. Mögliche Werte: • Microsoft • Junos Pulse • SonicWALL Mobile Connect • F5 • Check Point Mobile • Manuelle Verbindungsdefinition Der Standardwert ist „Microsoft“.
Server	Diese Einstellung gibt die öffentliche oder routbare IP-Adresse oder den DNS-Namen des VPN an. Diese Einstellung kann auf die externe IP eines VPN oder eine virtuelle IP einer Serverfarm hinweisen. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist.
Server-URL-Liste	Diese Einstellung gibt eine durch Kommas getrennte Liste von Servern mit URL, Hostname oder IP-Format an. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ nicht auf „Microsoft“ gesetzt ist.

Windows: VPN-Profileinstellung	Beschreibung
Typ der Routingrichtlinie	Diese Einstellung legt den Typ der Routingrichtlinie fest. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist. Mögliche Werte: • Split-Tunneling • Tunnel erzwingen Der Standardwert ist „Tunnel erzwingen“.
Nativer Protokolltyp	Diese Einstellung legt den Typ der Routingrichtlinie für das VPN fest. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ auf „Microsoft“ gesetzt ist. Mögliche Werte: • L2TP • PPTP • IKEv2 • Automatisch Der Standardwert ist „Automatisch“.
Authentifizierung	Diese Einstellung gibt die Authentifizierungsmethode für das systemeigene VPN an. Die Einstellung „Nativer Protokolltyp“ legt fest, welche Authentifizierungsmethoden unterstützt werden und welcher Standardwert für diese Einstellung verwendet wird: • Wenn Sie L2TP oder PPTP auswählen, sind die möglichen Werte „MS-CHAPv2“ und „EAP“. Der Standardwert ist „MS-CHAPv2“. • Wenn Sie IKEv2 auswählen, sind die möglichen Werte „Benutzermethode“ und „Gerätemethode“. Der Standardwert ist „Benutzermethode“. • Wenn Sie „Automatisch“ auswählen, ist der einzige mögliche Wert „EAP“. Mögliche Werte: • EAP • MS-CHAPv2 • Benutzermethode • Gerätemethode
EAP-Konfiguration	Diese Einstellung legt die XML der EAP-Konfiguration fest. Weitere Informationen zum Generieren der EAP-Konfigurations-XML finden Sie unter https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „EAP“ gesetzt ist.

Windows: VPN-Profileinstellung	Beschreibung
Benutzermethode	Diese Einstellung gibt an, dass der Typ „Benutzermethode“ zur Authentifizierung verwendet werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „Benutzermethode“ gesetzt ist. Mögliche Werte: • EAP
Gerätemethode	Diese Einstellung gibt an, dass der Typ „Gerätemethode“ zur Authentifizierung verwendet werden soll. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Authentifizierung“ auf „Gerätemethode“ gesetzt ist. Möglicher Wert: • Zertifikat
Benutzerdefinierte Konfiguration	Diese Einstellung gibt das HTML-codierte XML-Blob für eine SSL-VPN-Plug-In-spezifische Konfiguration an, einschließlich Authentifizierungsdaten, die an das Gerät gesendet werden, um sie für SSL-VPN-Plug-Ins verfügbar zu machen. Diese Einstellung ist nur dann gültig, wenn der „Verbindungstyp“ nicht auf „Microsoft“ gesetzt ist.
Name der Plug-In-Paketfamilie	Diese Einstellung legt den Namen der Paketfamilie des kundenspezifischen SSL-VPN fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Verbindungstyp“ auf „Manuelle Verbindungsdefinition“ gesetzt ist.
Vorinstallierter Schlüssel L2TP	Diese Einstellung legt den vorinstallierten Schlüssel für L2TP-Verbindungen fest.
App-Auslöserliste	Diese Einstellung gibt eine Liste von Apps an, mit welchen die VPN-Verbindung gestartet wird.
App-Auslöserliste > App-ID	Diese Einstellung gibt eine App für ein Per App VPN an. Mögliche Werte: • Name der Paketfamilie. Um den Namen der Paketfamilie zu erfahren, installieren Sie die App, und führen Sie den Windows PowerShell-Befehl `Get-AppxPackage` aus. Weitere Informationen finden Sie unter http://technet.microsoft.com/en-us/library/hh856044.aspx • Installationsort der App. Zum Beispiel C:\WINDOWS\System\notepad.exe.
Routenliste	Diese Einstellung gibt eine Liste von Routen an, die das VPN verwenden kann. Wenn das VPN Split-Tunneling verwendet, ist eine Routenliste erforderlich.
Subnetzadresse	Diese Einstellung gibt die IP-Adresse des Zielpräfixes im IPv4- oder IPv6-Adressformat an.

Windows: VPN-Profileinstellung	Beschreibung
Subnetzpräfix	Diese Einstellung gibt das Subnetzpräfix des Zielpräfixes an.
Ausschluss	Diese Einstellung gibt an, ob die hinzugefügte Weiterleitung auf eine VPN-Schnittstelle als Gateway oder eine physische Schnittstelle verweisen muss. Wenn Sie das Kontrollkästchen aktivieren, wird der Datenverkehr über die physische Schnittstelle geleitet. Wenn Sie das Kontrollkästchen nicht aktivieren, wird der Datenverkehr über das VPN geleitet.
Domänennamenliste	Diese Einstellung legt die NRPT-Regeln (Name Resolution Policy Table) für das VPN fest.
Domänenname	Diese Einstellung gibt den FQDN oder das Suffix der Domäne an.
DNS-Server	Diese Einstellung gibt die Liste der IP-Adressen der DNS-Server durch Kommas getrennt an.
Web-Proxyserver	Diese Einstellung gibt die IP-Adresse des Web-Proxyservers an.
VPN-Verwendung auslösen	Die Einstellung legt fest, ob diese Domänennamenregel die VPN-Verwendung auslöst.
Permanent	Diese Einstellung legt fest, ob die Domänennamenregel angewendet wird, wenn keine VPN-Verbindung besteht.
Filterliste für Verkehr	Diese Einstellung legt die Regeln fest, die Datenverkehr über das VPN zulassen.
Filterliste für Verkehr > App-ID	Diese Einstellung gibt eine App für einen App-basierten Verkehrsfilter an. Mögliche Werte: • Name der Paketfamilie. Um den Namen der Paketfamilie zu erfahren, installieren Sie die App, und führen Sie den Windows PowerShell-Befehl `Get-AppxPackage` aus. Weitere Informationen finden Sie unter http://technet.microsoft.com/en-us/library/hh856044.aspx • Installationsort der App. Zum Beispiel `C:\WINDOWS\System\notepad.exe`. • Geben Sie „SSYSTEM“ ein, um zu ermöglichen, dass der Kernel-Treiber Datenverkehr über das VPN sendet (z. B. PING oder SMB).
Protokoll	Diese Einstellung legt das vom VPN verwendete Protokoll fest. Mögliche Werte: • Alle • TCP • UDP Der Standardwert ist „Alle“.
Lokale Portbereiche	Diese Einstellung gibt die Liste der zulässigen lokalen Portbereiche getrennt durch Kommas an. Zum Beispiel 100-120, 200, 300-320.

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

Windows: VPN-Profileinstellung	Beschreibung
Authentifizierungstransformationskonstante	Mögliche Werte: • MD596 • SHA196 • SHA256128 • GCMAES128 • GCMAE192 • GCMAES256 Die Standardeinstellung ist „MD596“.
Chiffriertransformationskon	Mögliche Werte: • DES • DES3 • AES128 • AES192 • AES256 • GCMAES128 • GCMAES192 • GCMAES256 Die Standardeinstellung ist „DES“.
Verschlüsselungsmethode	Mögliche Werte: • DES • DES3 • AES128 • AES192 • AES256 Die Standardeinstellung ist „DES“.
Integritätsprüfungsmethode	Mögliche Werte: • MD5 • SHA196 • SHA256 • SHA384 Die Standardeinstellung ist „MD5“.

Windows: VPN-Profileinstellung	Beschreibung
Diffie-Hellman-Gruppe	Mögliche Werte: • Group1 • Group2 • Group14 • ECP256 • ECP384 • Group24 Die Standardeinstellung ist „Group1“.
PFS-Gruppe	Mögliche Werte: • PFS1 • PFS2 • PFS2048 • ECP256 • ECP384 • PFSMM • PFS24 Der Standardwert ist „PFS1“.
Proxy-Typ	Diese Einstellung legt den Typ der Proxy-Konfiguration für das VPN fest. Mögliche Werte: • Keine • PAC-Konfiguration • Manuelle Konfiguration Der Standardwert ist „Keine“.
PAC-URL	Diese Einstellung gibt die URL für den Webserver an, der die PAC-Datei hostet, einschließlich PAC-Dateinamen. Zum Beispiel http://www.example.com/PACfile.pac. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „PAC-Konfiguration“ gesetzt ist.
Adresse	Diese Einstellung legt den FQDN oder die IP-Adresse eines Proxy-Servers fest. Diese Einstellung ist nur dann gültig, wenn die Einstellung „Proxy-Typ“ auf „Manuelle Konfiguration“ gesetzt ist.
Verknüpftes SCEP-Profil	Diese Einstellung legt das verknüpfte SCEP-Profil fest, das ein Gerät verwendet, um ein Client-Zertifikat für die VPN-Authentifizierung abzurufen.

Per App VPN aktivieren

Sie können VPN pro App auf iOS-, iPadOS-, Samsung Knox- und Windows 10-Geräten einrichten, um zu bestimmen, welche Apps auf Geräten ein VPN für die Datenübertragung verwenden müssen. Per App VPN trägt zur Senkung der Belastung Ihres Unternehmens-VPN bei, indem nur bestimmter geschäftlicher Datenverkehr für die Verwendung des VPN freigegeben wird (bspw. Zugriff auf Anwendungsserver oder Webseiten hinter der Firewall). In lokalen Umgebungen unterstützt diese Funktion auch die Privatsphäre des Benutzers und erhöht die Verbindungsgeschwindigkeit für persönliche Apps, indem der persönliche Datenverkehr nicht über das VPN gesendet wird.

Für iOS- und iPadOS-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-Aktivierungen 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 VPN pro App-Einstellungen einer App auf iOS- und iPadOS-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-, iPadOS-, macOS- und Android-Geräte ein Proxy-Profil. Fügen Sie für Windows 10-Geräte die Proxy-Einstellungen im Wi-Fi- oder VPN-Profil hinzu.

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

Gerät	Proxy-Konfiguration
iOS und iPadOS	Erstellen Sie ein Proxy-Profil, und ordnen Sie es den von Ihrer Organisation verwendeten Profilen zu, zu denen folgende gehören können: • Wi-Fi • VPN Sie können auch den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Proxy-Profil zuweisen. **Hinweis:** Ein Proxy-Profil, das Benutzerkonten, Benutzergruppen oder Gerätegruppen zugewiesen wird, ist nur ein globaler Proxy für überwachte Geräte und hat Vorrang vor einem Proxy-Profil, das mit einem VPN- oder Wi-Fi-Profil verknüpft ist. Überwachte Geräte verwenden die globalen Proxy-Einstellungen für alle HTTP-Verbindungen.
macOS	Erstellen Sie ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi- oder VPN-Profil. Bei macOS gelten Profile für Benutzerkonten oder Geräte. Proxy-Profile gelten für Geräte.
Android	Erstellen Sie für Android Enterprise-Geräte ein Proxy-Profil, und verknüpfen Sie es mit einem Wi-Fi-Profil. 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.

Gerät	Proxy-Konfiguration
Samsung Knox	Erstellen Sie ein Proxy-Profil, und verknüpfen Sie es mit den Profilen, die Ihr Unternehmen nutzt. Es gelten folgende Bedingungen: • Für die Wi-Fi-Profile werden nur Proxy-Profile mit manueller Konfiguration auf Knox-Geräten unterstützt. Proxy-Profile, die Sie mit Wi-Fi-Profilen verknüpfen, unterstützen Proxy-Server, die eine allgemeine Authentifizierung, NTLM oder gar keine Authentifizierung verwenden. • Für VPN- und Enterprise-Konnektivitätsprofile werden Proxy-Profile mit manueller Konfiguration auf Samsung Knox-Geräten mit Android Enterprise-Aktivierungen und Samsung Knox Workspace-Geräten mit Knox 2.5 und höher unterstützt. Proxy-Profile mit PAC-Konfiguration werden auf Samsung Knox-Geräten mit Android Enterprise-Aktivierungen und Knox Workspace-Geräten mit Knox-Version höher als 2.5 unterstützt. **Hinweis:** Für die Verwendung eines Proxy-Profils mit einem Enterprise-Konnektivitätsprofil muss BlackBerry Secure Connect Plus aktiviert sein. Sie können auch den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen ein Proxy-Profil zuweisen. Es gelten folgende Bedingungen: • Auf Knox Workspace-Geräten und Samsung Knox-Geräten mit Android Enterprise-Aktivierungen bestimmt das Profil die Browser-Proxy-Einstellungen des geschäftlichen Bereichs. • Auf Samsung Knox-MDM-Geräten bestimmt die Profilkonfiguration die Browser-Proxy-Einstellungen des Geräts. **Hinweis:** PAC-Konfiguration wird auf Knox Workspace-Geräten mit Knox 2.5 und früher und Knox-MDM-Geräten nicht unterstützt.
Windows 10	Erstellen Sie ein Wi-Fi- oder VPN-Profil, und geben Sie die Proxy-Serverinformationen in den Profileinstellungen an. Es gelten folgende Bedingungen: • Wi-Fi-Proxy unterstützt nur manuelle Konfiguration und ist nur mit Windows 10 Mobile-Geräten kompatibel. • VPN-Proxy unterstützt PAC oder manuelle Konfiguration.

Erstellen eines Proxy-Profils

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	**a.** Vergewissern Sie sich, dass in der Dropdown-Liste **Typ** die Option **PAC-Konfiguration** ausgewählt ist. **b.** Geben Sie im Feld **PAC-URL** die URL für den Webserver an, der die PAC-Datei hostet, sowie den PAC-Dateinamen (zum Beispiel http://www.example.com/PACfile.pac). Die PAC-Datei sollte nicht auf einem Server gehostet werden, der BlackBerry UEM oder eine seiner Komponenten hostet. **c.** Führen Sie auf der Registerkarte **BlackBerry** die folgenden Aktionen aus: **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 **Benutzername** `%UserName%` ein. Wenn der Proxy-Server den Domänennamen zur Authentifizierung benötigt, verwenden Sie das Format *<domäne>**<benutzername>*. **2.** Klicken Sie in der Dropdown-Liste **Benutzerdefinierbar** auf die Proxy-Einstellungen, die die Benutzer von BlackBerry 10-Geräten ändern können. Die Standardeinstellung ist **Schreibgeschützt**.
Festlegen der Einstellungen zur manuellen Konfiguration	**a.** Klicken Sie in der Dropdown-Liste **Typ** auf **Manuelle Konfiguration**. **b.** Geben Sie im Feld **Host** den FQDN oder die IP-Adresse des Proxy-Servers ein. **c.** Geben Sie im Feld **Port** die Portnummer des Proxy-Servers ein. **d.** Wenn Ihr Unternehmen erfordert, dass Benutzer einen Benutzernamen und ein Kennwort für die Verbindung zum Proxy-Server eingeben, und das Profil für mehrere Benutzer gilt, geben Sie im Feld **Benutzername** `%UserName%` ein. Wenn der Proxy-Server den Domänennamen zur Authentifizierung benötigt, verwenden Sie das Format *<domäne>**<benutzername>*. **e.** Führen Sie auf der Registerkarte **BlackBerry** die folgenden Aktionen aus: **1.** Klicken Sie in der Dropdown-Liste **Benutzerdefinierbar** auf die Proxy-Einstellungen, die die Benutzer von BlackBerry 10-Geräten ändern können. Die Standardeinstellung ist **Schreibgeschützt**. **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 **Ausschlussliste** 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. *.beispiel.com oder 192.0.2.*) verwenden.

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

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

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

BlackBerry Secure Connect Plus und unterstützte Geräte erstellen einen sicheren IP-Tunnel, wenn dies die beste Wahl für eine Verbindung mit dem Netzwerk des Unternehmens ist. Ist einem Gerät ein Wi-Fi oder VPN-Profil zugewiesen, und das Gerät hat Zugriff auf das geschäftliche Wi-Fi- bzw. VPN-Netzwerk, wird diese Methode zum Herstellen einer Verbindung verwendet. Stehen diese Möglichkeiten nicht zur Verfügung (z. B. wenn der Benutzer sich außerhalb des geschäftlichen Wi-Fi-Funkbereichs befindet), stellen BlackBerry Secure Connect Plus und das Gerät einen sicheren IP-Tunnel her.

Wenn Sie auf iOS- und iPadOS-Geräten „VPN pro App“ 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 Infrastructure mit BlackBerry UEM. Für jedes Gerät wird ein Tunnel erstellt. Der Tunnel unterstützt Standard-IPv4-Protokolle (TCP und UDP), und der IP-Datenverkehr, der zwischen Geräten und 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	Vergewissern Sie sich, 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 Benutzerkonten oder Benutzergruppen 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 es sich, Per App VPN für BlackBerry Secure Connect Plus zu konfigurieren. Weitere Informationen zum BlackBerry Secure Gateway finden Sie unter Schützen von E-Mail-Daten mithilfe von BlackBerry Secure Gateway.

Unterstützte Geräte:

Gerät	Anforderungen
iOS und iPadOS	• Geräte müssen mit dem BlackBerry UEM Client aus dem App Store aktiviert werden. • MDM-Steuerelemente-Aktivierungsart

Android Enterprise	• Eine der folgenden Aktivierungsarten:
	  • Nur geschäftlicher Bereich (Premium)
	  • Geschäftlich und persönlich – vollständige Kontrolle (Premium)
	  • Geschäftlich und persönlich – Benutzer-Datenschutz (Premium)

Samsung Knox Workspace	• Samsung Knox MDM Version 5.0 oder höher
	• Samsung Knox Version 2.3 oder höher
	• Eine der folgenden Aktivierungsarten:
	  • Nur geschäftlicher Bereich (Samsung Knox)
	  • Geschäftlich und persönlich – vollständige Kontrolle (Samsung Knox)
	  • Geschäftlich und persönlich – Benutzer-Datenschutz (Samsung Knox)

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 den 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, wird BlackBerry Secure Connect Plus auf die neueste Version upgegradet.

Anweisungen zu Installation oder Upgrade von BlackBerry Connectivity Node finden Sie unter „Installation und Upgrade von BlackBerry Connectivity Node“ in der BlackBerry UEM CloudDokumentation zur Konfiguration. Sie müssen den 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 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-Diensten 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 unverfügbar wird, weist die BlackBerry Infrastructure das Gerät der anderen Instanz zu. Das Gerät nimmt die Verwendung des sicheren Tunnels mit minimaler Unterbrechung wieder auf.

Enable BlackBerry Secure Connect Plus

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

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

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

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 „VPN pro App“ für iOS- und iPadOS-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-, iPadOS-, Android Enterprise- und Knox Workspace-Geräten können die App zum Anzeigen des Verbindungsstatus öffnen. Es sind keine weiteren Maßnahmen von den Benutzern erforderlich.
- Wenn Sie mehrere Enterprise-Konnektivitätsprofile erstellt haben, weisen Sie ihnen eine Rangordnung zu.
- Wenn Sie ein Verbindungsproblem mit einem iOS-, iPadOS-, Android Enterprise- oder Knox Workspace-Gerät beheben müssen, kann der Benutzer Geräteprotokolle an die E-Mail-Adresse eines Administrators senden (der Benutzer gibt eine von Ihnen bereitgestellte E-Mail-Adresse an). Beachten Sie, dass die Anzeige der Protokolle mit Winzip nicht möglich ist. Es ist daher empfehlenswert, ein anderes Tool wie z. B. 7-Zip zu verwenden.

Enterprise-Konnektivitätsprofileinstellungen

Enterprise-Konnektivitätsprofile werden auf den folgenden Gerätetypen unterstützt:

- iOS
- iPadOS
- Android

Allgemein: Enterprise-Konnektivitätsprofileinstellungen

Allgemein: Einstellung für Kompatibilitätsprofil	Beschreibung
BlackBerry Secure Connect Plus-Servergruppe	Diese Einstellung gibt die Servergruppe an, die BlackBerry Secure Connect Plus zur Leitung des Datenverkehrs zu einem bestimmten regionalen Pfad verwendet. Diese Einstellung ist nur gültig, wenn Sie eine oder mehrere Instanzen von BlackBerry Connectivity Node installiert und Servergruppen eingerichtet haben.

iOS: Enterprise-Konnektivitätsprofileinstellungen

Einstellungen für iOS gelten auch für iPadOS-Geräte.

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

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

Android: Enterprise-Konnektivitätsprofileinstellungen

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

Einstellung	Beschreibung
Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich	Diese Einstellung gibt an, ob Android Enterprise- und Samsung Knox Workspace-Geräte BlackBerry Secure Connect Plus für alle Apps im geschäftlichen Bereich oder nur für bestimmte Apps verwenden. • „Containerweites VPN“ verwendet eine VPN-Verbindung für alle Apps im geschäftlichen Bereich auf dem Gerät. • „Per App VPN“ verwendet nur für die angegebenen Apps eine VPN-Verbindung.
Apps, die BlackBerry Secure Connect Plus nicht verwenden dürfen	Diese Einstellung gibt Apps im geschäftlichen Bereich auf Android Enterprise-Geräten an, die BlackBerry Secure Connect Plus nicht verwenden dürfen. Klicken Sie auf +, und geben Sie die App-Paket-ID ein. Wiederholen Sie den Vorgang bei Bedarf, um weitere Apps zu sperren. 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. Standardmäßig werden die Pakete dem neuen Enterprise-Konnektivitätsprofil hinzugefügt, Sie müssen sie jedoch allen vorhandenen Profilen hinzufügen. 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 support.blackberry.com/community im Artikel 48330. Wenn Ihr Unternehmen BlackBerry Dynamics-Apps verwendet, wird empfohlen, die Verwendung von BlackBerry Secure Connect Plus durch die Apps einzuschränken. Wenn nicht, müssen Sie zusätzliche Ports in der Firewall Ihres Unternehmens öffnen, damit die Apps Daten an den BlackBerry Dynamics NOC senden können. Die Netzwerkaktivität der Apps ist sonst eventuell verzögert, da die Daten sowohl zur BlackBerry Infrastructure als auch zu BlackBerry Dynamics NOC geleitet werden. Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise -Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Containerweites VPN“ gesetzt ist.
Apps, die Enterprise-Konnektivität verwenden dürfen	Diese Einstellung gibt Apps im geschäftlichen Bereich auf Android Enterprise- und Samsung Knox Workspace-Geräten an, die BlackBerry Secure Connect Plus verwenden dürfen. Sie können Apps aus einer Liste verfügbarer Apps auswählen oder die App-Paket-ID angeben. Diese Einstellung ist nur gültig, wenn die Einstellung „Enterprise-Konnektivität für Android-Geräte mit geschäftlichem Bereich“ auf „Per App VPN“ gesetzt ist.

Einstellung	Beschreibung
Proxyprofil	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 Proxy-Server zum geschäftlichen Netzwerk weiterleiten möchten, wählen Sie das entsprechende Proxy-Profil aus. 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.

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

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

Wenn Sie BlackBerry Secure Connect Plus aktivieren und eine lokale Umgebung mit BlackBerry Dynamics-Apps verwenden, die auf Android Enterprise-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**.

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*<jjjjmmtt>* 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*<JJJJMMTT>*.

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

Verwenden von BlackBerry 2FA für sichere Verbindungen mit kritischen Ressourcen

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

Die Verwaltung von BlackBerry 2FA erfolgt über die BlackBerry UEM-Verwaltungskonsole, in der Sie ein BlackBerry 2FA-Profil zum Aktivieren der Zwei-Faktor-Authentifizierung für Ihre Benutzer verwenden. Um die neueste Version von BlackBerry 2FA und die zugehörigen Funktionen nutzen zu können, z. B. Vorauthentifizierung und Wiederherstellung, muss den Benutzern das BlackBerry 2FA-Profil zugewiesen werden. Weitere Informationen finden Sie in der Dokumentation zu BlackBerry 2FA.

Einrichten einer Authentifizierung bei einmaliger Anmeldung für Geräte

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

Auf Geräten mit iOS oder iPadOS 13 und höher müssen Sie ein Profil für die SSO-Erweiterung verwenden, damit sich die Geräte automatisch bei Domänen und Webservices im Netzwerk Ihres Unternehmens authentifizieren können. Auf Geräten mit älteren Versionen als iOS 13 wurden SSO-Profile verwendet.

- Kerberos
- NTLM
- SCEP-Zertifikate für festgelegte vertrauenswürdige Domains

BlackBerry Dynamics-Apps unterstützen auch die Kerberos-Authentifizierung. Weitere Informationen finden Sie unter Konfigurieren von Kerberos für BlackBerry Dynamics-Apps.

SSO-Erweiterungsprofil erstellen

Single Sign-On-Erweiterungen werden auf Geräten mit iOS und iPadOS 13 und höher unterstützt. Sie können Einstellungen für eine benutzerdefinierte Erweiterung angeben oder die Kerberos-Erweiterung verwenden, die von Apple bereitgestellt wird.

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

1. Klicken Sie in der Menüleiste 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 in der Dropdown-Liste **Erweiterungstyp für einmalige Anmeldung** an, ob Sie eine benutzerdefinierte Erweiterung oder die von Apple bereitgestellte Kerberos-Erweiterung verwenden.

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

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

6. Klicken Sie auf **Speichern**.

Einrichten von DNS-Profilen für iOS- und macOS-Geräte

Sie können die DNS-Server angeben, die Sie für den Zugriff auf bestimmte Domänen verwenden möchten. Diese Einstellung kann dazu beitragen, das Surfen im Internet auf Geräten mit iOS und iPadOS 14 und höher sowie macOS 11 und höher zu beschleunigen und sicherer zu machen.

Erstellen eines DNS-Profils

1. Klicken Sie in der Menüleiste auf **Richtlinien und Profile**.
2. Klicken Sie auf **Netzwerke und Verbindungen > DNS**.
3. Klicken Sie auf +.
4. Geben Sie einen Namen und eine Beschreibung für das Profil ein.
5. Klicken Sie auf die Registerkarte eines Gerätetyps.
6. Wählen Sie das DNS-Protokoll für die Kommunikation mit dem DNS-Server aus.
7. Führen Sie einen der folgenden Schritte aus:
   a) Wenn Sie **HTTPS** ausgewählt haben, geben Sie die URI-Vorlage des DNS-over-HTTPS-Servers unter Verwendung des Schemas https:// ein.
   b) Wenn Sie **TLS** ausgewählt haben, geben Sie den Hostnamen des DNS-over-TLS-Servers ein.
8. Wählen Sie die Option **Nicht zulassen, dass Benutzer DNS-Einstellungen deaktivieren** aus, um zu verhindern, dass Benutzer diese Einstellungen deaktivieren. Diese Option wirkt sich nur auf überwachte Geräte aus.
9. Geben Sie im Feld **DNS-Adressen** die Liste der IP-Adressen für alle DNS-Server an, die Sie verwenden möchten. Dabei kann es sich um eine Mischung aus IPv4- und IPv6-Adressen handeln.
10. Geben Sie im Feld **Domänen** die Liste der Domänenzeichenfolgen an, die verwendet werden, um zu bestimmen, welche DNS-Abfragen die DNS-Server verwenden.
11. Geben Sie im Feld **Regeln für DNS-On-Demand** die DNS-On-Demand-Regeln mithilfe des Beispiels für das Payload-Format an.
12. Klicken Sie auf **Speichern**.
13. Wiederholen Sie die Schritte 5 bis 12 für jeden Gerätetyp.

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- und iPadOS-Geräte mit der Aktivierungsart „MDM-Steuerelemente“.

Nach dem Zuweisen eines Profils für verwaltete Domänen:

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

Erstellen eines Profils für verwaltete Domänen

Profile für verwaltete Domänen gelten nur für iOS- und iPadOS-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 Geräte unter Aufsicht 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- und iPadOS-Geräten das mobile Netzwerk nutzen.

Um die Netzwerkauslastung zu steuern, können Sie verhindern, dass die angegebenen Apps Daten übertragen, wenn die Geräte mit dem Mobilfunknetz verbunden sind oder sich im Roaming-Modus befinden. Ein Netzwerknutzungsprofil kann Regeln für eine App oder mehrere Apps enthalten.

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- oder iPadOS-Gerät unter Aufsicht aufrufen kann. Sie können den Benutzerkonten, den Benutzergruppen oder den Gerätegruppen Webinhaltsfilter-Profile zuweisen.

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

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

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	**a.** Vergewissern Sie sich, dass in der Dropdown-Liste **Zugelassene Websites** die Option **Nur bestimmte Websites** ausgewählt ist. **b.** Klicken Sie im Abschnitt **Lesezeichen für bestimmte Websites** auf +. **c.** Führen Sie folgende Aktionen aus: **1.** Geben Sie im Feld **URL** eine Webadresse ein, für die der Zugriff gestattet werden soll. **2.** Optional können Sie auch im Feld **Lesezeichenpfad** den Namen eines Lesezeichenordners eingeben (zum Beispiel: /Work/). **3.** Geben Sie im Feld **Titel** einen Namen für die Website ein. **4.** Klicken Sie auf **Hinzufügen**. **d.** Wiederholen Sie die Schritte 2 und 3 für alle zugelassenen Websites.
Beschränken von nicht jugendfreien Inhalten	**a.** Klicken Sie in der Dropdown-Liste **Zugelassene Websites** auf **Nicht jugendfreie Inhalte beschränken**, um die automatische Filterung zu aktivieren. **b.** Führen Sie optional folgende Aktionen aus: **1.** Klicken Sie auf + neben **Erlaubte URLs**. **2.** Geben Sie eine Webadresse ein, für die der Zugriff gewährt werden soll. **3.** Wiederholen Sie für jede zugelassene Website die Schritte 2.a und 2.b. **c.** Führen Sie optional folgende Aktionen aus: **1.** Klicken Sie auf + neben **Gesperrte URLs**. **2.** Geben Sie eine Webadresse ein, für die der Zugriff nicht gewährt werden soll. **3.** Wiederholen Sie für jede beschränkte Website die Schritte 3.a und 3.b.

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 BonjourAirPrint-fähige Drucker in einem anderen Subnetzwerk nicht erkennen können, können Sie mithilfe von AirPrint-Profilen angeben, wo sich die entsprechenden Ressourcen befinden. Sie können AirPrint-Profile iOS- und iPadOS-Geräten zuweisen, damit Benutzer Drucker nicht manuell konfigurieren müssen.

Bei AirPlay handelt es sich um eine AirPlay-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 festlegen, zu welchen AirPlay-Geräten Benutzer von iOS und iPadOS eine Verbindung herstellen können. Das AirPlay-Profil bietet zwei Optionen an:

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

Erstellen eines AirPrint-Profils

Sie können AirPrint-Profile konfigurieren und sie iOS- und iPadOS-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 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 `_ipps.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**.
9. Wenn sich der Port vom Standard für das Internet Printing Protocol unterscheidet, geben Sie optional die Portnummer in das Feld **Port** ein.

10. Klicken Sie auf **Hinzufügen**.
11. Klicken Sie auf **Hinzufügen**.

Erstellen eines AirPlay-Profils

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, für das Sie das Kennwort bereitstellen möchten. Sie können den Namen des AirPlay-Geräts in den Geräteeinstellungen suchen, oder Sie können den Namen des Geräts durch Tippen auf **Airplay** im Control Center eines iOS- oder iPadOS-Geräts suchen, wodurch eine Liste der verfügbaren AirPlay-Geräte in Ihrer Nähe aufgeführt wird.
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 des AirPlay-Geräts ein, mit dem sich überwachte Geräte verbinden können. Sie können die Geräte-ID für das AirPlay-Gerät in den Geräteeinstellungen finden. Überwachte Geräte können nur mit AirPlay-Geräten in der Liste verbunden werden.
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 und höher mit Nur geschäftlicher Bereich-Aktivierungen und von Geräten mit Android 9 und 10 mit Geschäftlich und persönlich – vollständige Kontrolle-Aktivierungen unterstützt.

In der Regel sind APNs für gängige Betreiber bereits auf den Geräten voreingestellt. Benutzer können einem Gerät auch neue APNs hinzufügen. Wenn Sie ein Gerät zwingen möchten, einen APN zu verwenden, der von einem APN-Profil an das Gerät gesendet wird, wählen Sie die IT-Richtlinienregel „Gerät zur Verwendung der APN-Profileinstellungen zwingen“ in den Android Global-IT-Richtlinienregeln (alle Android-Geräte) aus.

Erstellen eines APN-Profils

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	Diese Einstellung legt die Datenkommunikationstypen fest, die diese APN-Konfiguration verwenden. Unterschiedliche Datenkommunikationstypen können unterschiedliche Konfigurationen verwenden. Mögliche Werte: • Standard-Datenverkehr • MMS-Datenverkehr • SUPL-unterstütztes GPS • DUN-Datenverkehr • Datenverkehr mit hoher Priorität • FOTA-Portal des Netzbetreibers • IMS • CBS • IA Initial Attach APN • Emergency PDN • MCX (Mission Critical Service)
Proxyadresse	Diese Einstellung gibt den HTTP-Proxy an, der für den gesamten Webverkehr über die Verbindung verwendet werden soll. Diese Einstellung ist für die meisten Netzbetreiber nicht erforderlich.
Proxy-Port	Diese Einstellung gibt den HTTP-Proxyport an, der für den gesamten Webverkehr über die Verbindung verwendet werden soll. Diese Einstellung ist für die meisten Netzbetreiber nicht erforderlich.
MMSC	Diese Einstellung legt das Multimedia Messaging Service Center (MMSC) für das Senden und Empfangen von MMS-Nachrichten fest.
MMS-Proxyadresse	Diese Einstellung legt den HTTP-Proxy für die Kommunikation mit dem MMSC zum Senden und Empfangen von MMS-Nachrichten fest.
MMS-Proxyport	Diese Einstellung legt den HTTP-Proxyport für die Kommunikation mit dem MMSC zum Senden und Empfangen von MMS-Nachrichten fest.
Authentifizierungstyp	Diese Einstellung gibt den für die Kommunikation verwendeten Authentifizierungstyp an. Mögliche Werte: • NONE • PAP • CHAP • PAP oder CHAP
Benutzername	Wenn die Einstellung „Authentifizierungstyp“ auf einen anderen Wert als NONE festgelegt ist, geben Sie einen Benutzernamen an, wenn er für die Authentifizierung erforderlich ist.

Einstellungen für APN-Profil	Beschreibung
Kennwort	Wenn die Einstellung „Authentifizierungstyp“ auf einen anderen Wert als NONE festgelegt ist, geben Sie ein Kennwort an, wenn es für die Authentifizierung erforderlich ist.
Mobile Country Code (MCC)	Diese Einstellung legt den Mobile Country Code für das Netzwerk des Netzbetreibers fest, für das die APN-Konfiguration verwendet werden soll.
Mobile Network Code (MNC)	Diese Einstellung legt den Mobile Network Code für das Netzwerk des Netzbetreibers fest, für das die APN-Konfiguration verwendet werden soll.
Protokoll	Diese Einstellung legt fest, ob IPv4, IPv6 oder beide im Heimnetzwerk für Geräte aktiviert werden sollen, die IPv6-Netzwerke unterstützen. Mögliche Werte: • IP • IPV6 • IPV4V6 • PPP
Roaming-Protokoll	Diese Einstellung legt fest, ob IPv4, IPv6 oder beides beim Roaming für Geräte aktiviert werden soll, die IPv6-Netzwerke unterstützen. Mögliche Werte: • IP • IPV6 • IPV4V6 • PPP
Betreiber-aktiviert	Diese Einstellung legt fest, ob der APN für den Betreiber aktiviert ist.
MVNO-Typ	Diese Einstellung legt fest, ob die Nutzung dieses APN auf bestimmte MVNOs (Mobilfunknetzhändler) oder Abonnentenkonten beschränkt werden soll. Mögliche Werte: • SP • IMSI • GID • ICCID

Rechtliche Hinweise

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

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

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

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

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

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

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

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

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

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

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

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

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

Veröffentlicht in Kanada