

BLACKBERRY ENTERPRISE

SERVICE 10

Device Management für iOS, Android und BlackBerry

Jetzt mit Support für iOS7 und Android 4.3

BlackBerry Enterprise Service 10 (BES10) ist eine einheitliche Plattform für das Device, Application und Content Management in heterogenen mobilen Umgebungen. Zuverlässige Sicherheit und stabile Konnektivität sind bereits integriert. Mit BES10 können Sie Ihren gesamten Bestand an mobilen Geräten sicher und effektiv verwalten.

Ob Firmen- oder Privatgeräte, ob mit iOS, Android™ oder BlackBerry: BES10 verwaltet alle Geräte über eine zentrale Management-Konsole.

BlackBerry® hat das Enterprise Mobility Management spektakulär vereinfacht. Mit der perfekten Kombination aus:

Mobile Device Management

BES10 bietet umfassende Verwaltung und Sicherheitskontrollen für firmeneigene und private iOS-, Android- und BlackBerry Geräte.

Höchste mobile Sicherheit

Das bewährte BlackBerry® Sicherheitsmodell gibt es jetzt auch auf iOS- und Android-Geräten. Für den optimalen Schutz geschäftlicher Inhalte auf dem Gerät und während der Datenübertragung.

Enterprise Application Management

Dies ist der einfachste Weg, um Mitarbeitern Apps zur Verfügung zu stellen: Einsatz, Verwaltung und Schutz von Apps für Nutzer von iOS, Android und BlackBerry erfolgen über eine einheitliche BES10 Konsole.



BES10 auf einen Blick

Benutzerfreundliche und intuitive Management-Konsole für die umfassende Verwaltung von Geräten, Sicherheit und Applikationen in heterogenen mobilen Umgebungen

Trennung von geschäftlichen und persönlichen Inhalten zum Schutz vor Datenverlust, Benutzerfreundlichkeit und Privatsphäre bleiben gewahrt

Flexible Sicherheitsstufen für Unternehmen und Anwender

Modernes Application Management für den einfachen Einsatz und die Verwaltung von Applikationen

Monitoring und Reporting von Geräten zur Erfüllung der Compliance-Vorschriften

Standardmäßig integrierter Support für eine hochwertige mobile IT

BlackBerry®

BlackBerry Enterprise Mobility Management können Sie passgenau implementieren:

Corporate EMM – Kontrollen und Einstellungen für Unternehmen jeder Größe:

BlackBerry bietet Ihnen umfassendes Device Management, Sicherheit und Application Management für firmeneigene und private iOS-, Android- und BlackBerry Geräte.

Alles über eine einzige End-to-End-Plattform von BES10. Sichern Sie sich jetzt die bewährte BlackBerry Sicherheit und Kontrolle für alle Geräte, die weit über die Möglichkeiten von ActiveSync hinausgehen.

BES10 sorgt für die nahtlose Trennung von geschäftlichen und persönlichen Inhalten. So erfüllt es die Erwartungen der Anwender und die Anforderungen der Unternehmen gleichermaßen.

Profitieren Sie von den zukunftsweisenden Eigenschaften des App Managements: von umfassenden Einsatzmöglichkeiten, der einfachen Verwaltung und höchster Sicherheit beim Umgang mit Applikationen. So können Sie vorgeschriebene Apps schnell und einfach pushen und installieren. Und dem Nutzer empfohlene Apps über einen Firmen-App-Store im geschäftlichen Bereich auf allen Geräten zur Verfügung stellen. Die Apps und Inhalte im persönlichen Bereich bleiben unangetastet.

Regulated EMM – Kontrollen und Einstellungen für Regierungsstellen und andere regulierte Umgebungen

Sie suchen ultimative Sicherheit? Mit dem Regulated Enterprise Mobility Management für iOS-, Android- und BlackBerry Geräte können Regierungsstellen und andere regulierte Umgebungen strenge Compliance-Vorschriften mühelos einhalten.

Sie müssen detaillierte Kontrollrichtlinien für Inhalte und Apps erfüllen? Auf Privat- und Firmengeräten? Dann ist BES10 ideal für Sie. Denn BES10 ist die ultimative Device Management Solution mit höchster Sicherheit bei der Mobilität.

Spezifische Kontrollen und Einstellungen für Regulated EMM finden Sie in einem separaten Datenblatt.

Erfüllt sämtliche Sicherheitsanforderungen: vom Basisschutz bis hin zum höchsten Sicherheitsniveau für Regierungsstellen und regulierte Umgebungen

	Abgestuftes Enterprise Mobility Management				
	Teilweise verwaltet	Komplett verwaltet	Abteilungsabhängige IT-Richtlinien	Mischung aus gesperrt und verwaltet	100% gesperrt
Regulated Device Management			■	■	■
Corporate Device Management	■	■	■	■	
Unternehmensart	Kleine und mittlere Unternehmen, die keine gesperrten Geräte brauchen.	Mittlere und große Unternehmen, die keine gesperrten Geräte brauchen.	Große Unternehmen mit unterschiedlichen Anforderungen beim Device Management.	Große Unternehmen mit hohem Sicherheitsbewusstsein.	Regierungsstellen und regulierte Branchen





Secure Work Space

Durch Containerisation, Application Wrapping und sichere Konnektivität haben wir einen Secure Work Space für Sie geschaffen, der Ihnen ein Höchstmaß an Kontrolle und Sicherheit für iOS- und Android-Geräte bietet. All das können Sie über die BES10 Management-Konsole verwalten.

Geschäftliche Applikationen bleiben geschützt und strikt von persönlichen Apps und Daten getrennt. Hierzu gehören eine integrierte App für E-Mail, Kalender und Kontakte, ein sicherer Browser sowie Documents To Go zum sicheren Ansehen und Bearbeiten von Dokumenten.

Für den Zugriff auf geschützte Apps ist eine Authentifizierung des Nutzers erforderlich. Geschäftliche Daten können außerhalb des Secure Work Space nicht geteilt werden.

Das bewährte BlackBerry Sicherheitsmodell bietet Ihnen sichere Konnektivität für alle Apps, die im Secure Work Space eingesetzt werden – kein VPN nötig.



BlackBerry Balance

Von der BlackBerry® Balance™ Technologie profitieren Sie und Ihr Unternehmen. Ihnen bietet sie Freiheit und Privatsphäre, Ihrem Unternehmen Sicherheit und Verwaltungsfunktionen. Diese perfekte Kombination ist in jedem BlackBerry 10 Smartphone integriert und wird über BES10 verwaltet.

Persönliche Applikationen und Informationen bleiben strikt von geschäftlichen getrennt. Der Wechsel zwischen den Bereichen gelingt leicht: Eine einfache Wischgeste genügt.

Dabei bleibt der geschäftliche Bereich jederzeit verschlüsselt, verwaltet und gesichert. So kann Ihr Unternehmen sensible Inhalte und Applikationen schützen, während Sie das volle Potenzial Ihres Smartphones im persönlichen Bereich nutzen können.

Corporate BlackBerry Device Management

Kontrollen und Einstellungen

Allgemein

Roaming

Legen Sie fest, ob ein BlackBerry Gerät während des Roamings Datendienste über das Mobilfunknetz nutzen darf.

Mobiler Hotspot-Modus und Tethering

Legen Sie fest, ob ein BlackBerry Gerät als mobiler Hotspot oder zum Tethering über Bluetooth-Technologie oder ein USB-Kabel verwendet werden darf.

Plans Applikation

Legen Sie fest, ob die Plans App auf dem BlackBerry Gerät laufen darf.

Mobilfunkrechnung

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts über den Firmentarif Ihres Mobilfunkanbieters Applikationen aus der BlackBerry App World kaufen kann.

Passwort

Mindestlänge

Legen Sie fest, wie viele Zeichen das Passwort für ein BlackBerry Gerät haben soll.

Sicherheits-Time-out

Legen Sie fest, wie viele Minuten vergehen dürfen, bis ein BlackBerry Gerät bei Inaktivität des Nutzers gesperrt wird.

Laufzeit

Legen Sie fest, wie viele Tage es dauert, bis ein Passwort auf einem BlackBerry Gerät ungültig wird und der Nutzer ein neues Passwort erstellen muss.

Komplexität

Legen Sie fest, wie komplex das Passwort auf einem BlackBerry Gerät sein soll.

Maximale Eingabeversuche

Legen Sie fest, wie oft ein Nutzer ein falsches Passwort auf einem BlackBerry Gerät eingeben darf, bevor alle Daten aus dem geschäftlichen Bereich automatisch gelöscht werden.

Historie

Legen Sie fest, wie viele alte Passwörter ein BlackBerry Gerät überprüft, um den Nutzer davor zu schützen, ein bereits genutztes Passwort erneut zu verwenden.

Passwortpflicht für den geschäftlichen Bereich

Legen Sie fest, ob ein BlackBerry Gerät ein Passwort für den geschäftlichen Bereich braucht.

Passwortpflicht für das gesamte Gerät

Legen Sie ein Passwort für das gesamte Gerät und den geschäftlichen Bereich fest. Der geschäftlichen Bereich auf dem Gerät kann – nach wie vor – unabhängig davon gesperrt werden.

Sicherheit

Geschäftlichen Bereich ohne Netzwerkverbindung löschen

Legen Sie fest, wie viele Stunden ein BlackBerry Gerät nicht mit dem Netzwerk Ihres Unternehmens verbunden sein darf, bevor alle Daten aus dem geschäftlichen Bereich gelöscht werden.

Zugriff für den Entwicklungsmodus auf den geschäftlichen Bereich

Legen Sie fest, ob der Entwicklungsmodus genutzt werden kann. Ob sich Tools zur Software-Entwicklung mit dem geschäftlichen Bereich auf dem BlackBerry Gerät über eine USB- oder Wi-Fi-Verbindung verbinden können, um Apps direkt im geschäftlichen Bereich zu installieren.

Sprachsteuerung

Legen Sie fest, ob ein Nutzer die Sprachbefehle auf einem BlackBerry Gerät nutzen darf.

Diktierfunktion in geschäftlichen Apps

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts die Diktierfunktion in geschäftlichen Apps nutzen darf.

Diktierfunktion

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts die Diktierfunktion auf einem Gerät nutzen darf.

Geschäftlichen Bereich mit der BlackBerry Desktop Software sichern und wiederherstellen

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts die Applikationen und Daten aus dem geschäftlichen Bereich des Geräts mit der BlackBerry Desktop Software sichern und wiederherstellen kann.

BlackBerry Bridge

Legen Sie fest, ob ein BlackBerry 10 Smartphone ein BlackBerry PlayBook Tablet nutzen kann, um über die BlackBerry Bridge App auf geschäftliche Daten auf dem Smartphone zuzugreifen.

Smart Card Passwort zwischenspeichern

Legen Sie fest, ob ein BlackBerry Gerät das Passwort einer Smart Card zwischenspeichern kann. (Smart Card Reader)

Intelligente Passwort-Eingabe

Legen Sie fest, ob ein Smart Card Passwort zwischengespeichert werden kann.

Sperrung bei Entfernung der Smart Card

Legen Sie fest, ob sich das BlackBerry Gerät sperrt, wenn der Nutzer die Smart Card aus einem unterstützten Smart Card Reader entfernt oder einen unterstützten Smart Card Reader vom BlackBerry Gerät trennt.

Maximale Bluetooth-Reichweite

Legen Sie fest, welche Reichweite ein Smart Card Reader für das Senden von Bluetooth-Paketen nutzen darf. Der Wert darf dabei zwischen 30 % (kürzeste Reichweite) und 100 % (längste Reichweite) liegen.

Mindestanforderungen PIN-Eingabe

Legen Sie fest, welche Mindestanforderungen für die PIN-Eingabe gelten, wenn ein BlackBerry Smart Card Reader mit einem BlackBerry Gerät oder Computer gekoppelt wird.

Sicherheits-Timer zurücksetzen

Legen Sie fest, ob Apps den Sicherheits-Timer auf einem BlackBerry Gerät zurücksetzen können. Damit wird verhindert, dass das Gerät bei Inaktivität des Nutzers durch das festgelegte Sicherheits-Time-out gesperrt wird. Der Nutzer kann dies auch über die Passwortsperre auf dem Gerät einstellen.

Datenverschlüsselung im persönlichen Bereich

Legen Sie fest, ob die Datenverschlüsselung für den persönlichen Bereich auf einem BlackBerry PlayBook Tablet eingeschaltet ist.

Kontrolle des Netzwerkzugriffs für geschäftliche Applikationen

Legen Sie fest, ob sich geschäftliche Applikationen auf einem BlackBerry Gerät über BlackBerry Enterprise Service 10 mit dem Netzwerk Ihres Unternehmens verbinden müssen.

Zugriff persönlicher Applikationen auf geschäftliche Kontakte

Legen Sie fest, ob persönliche Applikationen (also Applikationen, die sich im persönlichen Bereich befinden) auf geschäftliche Kontakte auf dem BlackBerry Gerät zugreifen können.

Teilen geschäftlicher Daten während BBM Video Screen Sharing

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts geschäftliche Daten (also Daten, die sich im geschäftlichen Bereich befinden) mit der Option BBM Video Screen Sharing auf einem Gerät teilen darf.

Zugriff geschäftlicher Applikationen auf persönliche Daten

Legen Sie fest, ob geschäftliche Applikationen auf einem BlackBerry Gerät auf persönliche Daten zugreifen dürfen, wenn der Nutzer dies erlaubt.

Geschäftliche Domains

Legen Sie eine Liste von Domainnamen fest, die ein BlackBerry Gerät als geschäftliche Ressourcen identifiziert. Gilt nur für die Print To Go App.

Geschäftliche Netzwerknutzung für persönliche Applikationen

Legen Sie fest, ob Applikationen aus dem persönlichen Bereich auf einem BlackBerry Gerät das Wi-Fi- oder VPN-Netzwerk Ihres Unternehmens nutzen dürfen, um sich mit dem Internet zu verbinden.

Zweifache Authentifizierung im geschäftlichen Bereich

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts die Zwei-Wege-Authentifizierung nur für den geschäftlichen Bereich nutzen kann.

Vorschau auf geschäftliche Inhalte bei gesperrtem Bildschirm

Legen Sie fest, ob ein BlackBerry Gerät geschäftliche Inhalte auf dem gesperrten Bildschirm anzeigt, wenn der geschäftliche Bereich im Hintergrund entsperrt ist.*

IRM-geschützte E-Mail-Nachrichten

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts IRM-geschützte Nachrichten lesen kann.*

Informationen zum Eigentümer

Legen Sie die Informationen zum Eigentümer oder eine Disclaimer-Nachricht auf dem gesperrten Bildschirm eines gesperrten Geräts fest.*

Persönliche Nachrichten weiterleiten oder Empfänger hinzufügen

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts eine Nachricht weiterleiten oder neue Empfänger hinzufügen kann, wenn die E-Mail-Nachricht als privat gekennzeichnet ist.*

Warnmeldung bei externen E-Mail-Adressen

Legen Sie fest, ob ein BlackBerry Gerät eine Warnmeldung anzeigt, wenn ein Nutzer eine geschäftliche E-Mail an einen externen Empfänger verschicken will.*

Liste erlaubter externer E-Mail-Domains

Legen Sie eine Liste externer E-Mail-Domains fest, an die der Nutzer eines BlackBerry Geräts geschäftliche E-Mails schicken darf, ohne dass auf dem Gerät eine Warnmeldung erscheint.*

Liste nicht erlaubter externer E-Mail-Domains

Legen Sie eine Liste externer E-Mail-Domains fest, an die der Nutzer eines BlackBerry Geräts keine geschäftlichen E-Mails schicken darf.*

Software

Öffnen von Links in geschäftlichen E-Mails im persönlichen Browser

Legen Sie fest, ob der Nutzer eines BlackBerry Geräts den Browser aus seinem persönlichen Bereich nutzen kann, um Links aus geschäftlichen E-Mails damit zu öffnen.

Einheitliche Ansicht für geschäftliche und persönliche Konten und Nachrichten

Legen Sie fest, ob die Nachrichten-Applikation auf dem BlackBerry Gerät Nachrichten von geschäftlichen und persönlichen Konten in einer Ansicht anzeigt.

Geschäftliche Kontakte mit Bluetooth PBAP oder HFP übertragen

Legen Sie fest, ob ein BlackBerry Gerät geschäftliche Kontakte über das Bluetooth Phone Book Access Profile (PBAP) oder Hands-Free Profile (HFP) auf ein anderes Bluetooth-fähiges Gerät schicken darf.

Geschäftliche Daten mit Bluetooth OPP übertragen

Legen Sie fest, ob ein BlackBerry Gerät über das Bluetooth Object Push Profile (OPP) geschäftliche Dateien an ein anderes Bluetooth- oder NFC-fähiges Gerät schicken darf.

Geschäftliche Daten mit NFC übertragen

Legen Sie fest, ob ein BlackBerry Gerät über NFC geschäftliche Daten an ein anderes NFC-fähiges Gerät schicken darf.

Geschäftliche Nachrichten mit Bluetooth MAP übertragen

Legen Sie fest, ob ein BlackBerry Gerät über das Bluetooth Message Access Profile (MAP) Nachrichten aus dem geschäftlichen Bereich (zum Beispiel E-Mails oder Instant Messages) auf ein anderes Bluetooth-fähiges Gerät schicken darf.

Zugriff von BBM Video auf das geschäftliche Netzwerk

Legen Sie fest, ob die Video Chat App auf einem BlackBerry Gerät das Wi-Fi- bzw. VPN-Netzwerk Ihres Unternehmens oder den BlackBerry MDS Connection Service für Video Chats nutzen kann.

Datenanalyse für Smart Calling

Legen Sie fest, ob ein BlackBerry Gerät Kontakt- und Gerätedaten zur Analyse an BlackBerry schicken darf. Mit den Ergebnissen kann das Gerät die beste Methode für den Anruf eines Kontakts empfehlen. Basierend auf den Informationen zum Gerät des Nutzers und des Kontakts und der Sprachqualität.

Protokollierung

Log Submission

Legen Sie fest, ob ein BlackBerry Gerät Logfiles generieren und an das BlackBerry Technical Solution Center schicken darf.

CCL Datensammlung

Legen Sie fest, ob ein BlackBerry Gerät die Datensammlung mittels Context Collection Library (CCL) über alle Apps hinweg erlaubt.

Bitte beachten Sie, dass die auf dieser Seite erwähnten Funktionen nur für BlackBerry 10 Geräte und BlackBerry Enterprise Service 10 gelten.

Informationen zum Device Management für firmeneigene und private iOS- und Android™-Geräte finden Sie auf der Rückseite.

*BlackBerry 10 Gerät mit 10.2.1 Gerätecode erforderlich



Corporate Device Management für iOS und Android™ Kontrollen und Einstellungen

iOS

Browser

Standard-Browser ausblenden
Autofill im Standard-Browser deaktivieren
Cookies deaktivieren
Betrugswarnungen im Standard-Browser deaktivieren
JavaScript im Standard-Browser deaktivieren
Pop-ups im Standard-Browser deaktivieren

Kamera und Video

Ausgabe deaktivieren
Bilderfassung deaktivieren
Standard-Kamera-Applikation ausblenden
Standard-Videokonferenz-Applikation ausblenden

Zertifikate

Nicht vertrauenswürdige Zertifikate deaktivieren
Nicht vertrauenswürdige Zertifikate nach Aufforderung deaktivieren
Mobile Updates von Zertifikaten deaktivieren

Cloud Service

Cloud Services deaktivieren
Cloud Back-up Service deaktivieren
Cloud Document Services deaktivieren
Cloud Picture Services deaktivieren
Cloud Picture Sharing Services deaktivieren

Verbindungsoptionen

Netzwerkverbindung deaktivieren
Drahtlose Verbindung deaktivieren
Roaming deaktivieren
Datendienste beim Roaming deaktivieren
Hintergrund-Datendienste beim Roaming deaktivieren
Sprachdienste beim Roaming deaktivieren
AirDrop deaktivieren
Änderungen bei der mobilen Datennutzung von Apps deaktivieren

Inhalt

Inhalt deaktivieren
Bestimmte Inhalte ausblenden
Contentfilter Jugendschutz für Applikationen
Contentfilter Jugendschutz für Filme
Contentfilter Jugendschutz für TV-Sendungen
Contentfilter Jugendschutz wird regional bestimmt

Diagnose und Nutzung

Versand von Diagnose-Logs an den Gerätehersteller deaktivieren

Messaging

Standard-Messaging-Applikation ausblenden

Bildschirm sperren

Tagesansicht bei gesperrtem Bildschirm ausblenden
Notification Center bei gesperrtem Bildschirm ausblenden
Control Center bei gesperrtem Bildschirm ausblenden

Sicherheit

Änderungen an Konten auf dem Gerät deaktivieren
Touch ID zum Entsperren des Geräts deaktivieren
Ad Tracking beschränken
Persönliche Daten in persönlichen Apps und Konten beschränken
Geschäftliche Daten in geschäftlichen Apps und Konten beschränken

Onlineshop

Onlineshops deaktivieren
Käufe in Applikationen deaktivieren
Speichern von Passwörtern für Onlineshops deaktivieren
Standard-Onlineshop für Applikationen ausblenden
Standard-Onlineshop für Bücher ausblenden
Kauf von Erotikwaren im Standard-Onlineshop für Bücher deaktivieren
Standard-Onlineshop für Musik ausblenden

Passbook Applikation

Passbook-Benachrichtigungen deaktivieren, wenn das Gerät gesperrt ist

Passwort

Passwortheigenschaften definieren
Wiederholung und einfache Muster vermeiden
Buchstaben verlangen
Zahlen verlangen
Sonderzeichen verlangen
Nach einer bestimmten Anzahl von falschen
Passwortheingaben die Daten und Applikationen auf dem
Gerät löschen
Gerätepasswort
Automatische Sperre aktivieren (Zeit, in der ein
gesperrtes Geräte ohne Eingabe eines Passworts wieder
entsperrt werden kann)
Laufzeit des Passworts beschränken
Passwort-Historie beschränken
Passwortlänge begrenzen
Mindestlänge für das Gerätepasswort festlegen

Telefon und Messaging

Sprachwahl deaktivieren

Profile und Zertifikate

Interaktive Installation von Profilen und Zertifikaten deaktivieren

Soziale Netzwerke

Soziale Netzwerke deaktivieren
Social Gaming deaktivieren
Hinzufügen von Freunden in der Standard-Social-
Gaming-Applikation deaktivieren
Gaming-Funktionalität für mehrere Spieler ausblenden
Standard-Social-Gaming-Applikation ausblenden
Standard-Social-Video-Applikation ausblenden
Änderungen bei den Einstellungen für „Meine Freunde
finden“ deaktivieren

Speichern und Back-up

Geräte-Back-up deaktivieren
Verschlüsselung für die Back-up-Daten eines Geräts verlangen

Sprachassistent

Standard-Applikation für Sprachassistent deaktivieren
Applikation für Sprachassistent deaktivieren, wenn das
Gerät gesperrt ist
Nutzergenerierte Inhalte in Applikationen für
Sprachassistent ausblenden

Android

Kamera und Video

Standard-Kamera-Applikation ausblenden

Passwort

Passwortheinstellungen festlegen
Buchstaben verlangen
Kleinbuchstaben verlangen
Zahlen verlangen
Sonderzeichen verlangen
Großbuchstaben verlangen
Nach einer bestimmten Anzahl von falschen
Passwortheingaben die Daten und Applikationen auf dem
Gerät löschen
Gerätepasswort
Automatische Sperre aktivieren
Laufzeit des Passworts beschränken
Passwort-Historie beschränken
Passwortlänge begrenzen
Mindestlänge für das Gerätepasswort festlegen

Verschlüsselung

Regeln zur Verschlüsselung anwenden
Intern auf dem Gerät gespeicherte Daten verschlüsseln

TouchDown Support

BES10 bietet Ihnen mit TouchDown™-Integration eine Lösung zur Synchronisation von Microsoft Exchange auf der Android™-Plattform. Die Integration ermöglicht das Senden von E-Mail-Profilen auf Android™-Geräte. Der BlackBerry Enterprise Service 10 Client erkennt den BES10 TouchDown Client auf dem Telefon des Anwenders und konfiguriert ihn automatisch, um die in BES10 zugewiesenen ActiveSync™-Profile zu nutzen.

ActiveSync™ Gatekeeping

BlackBerry Enterprise Service 10 kann so konfiguriert werden, dass es den Zugriff auf Microsoft® Exchange Server 2010 für verwaltete iOS- und Android™-Geräte kontrolliert. Verwaltete Geräte, die mit den in BlackBerry Enterprise Service 10 definierten Compliance-Richtlinien übereinstimmen, werden automatisch zur genehmigten Liste auf der Exchange Mailbox des Geräts hinzugefügt. Geräte, für die das nicht gilt, können nicht auf Microsoft® ActiveSync™ zugreifen.

**Weitere Informationen zu
BlackBerry Enterprise Service 10
finden Sie unter www.BES10.com.**

 **BlackBerry®**

Android ist eine Marke von Google Inc.

iOS ist eine eingetragene Marke von Cisco Systems, Inc. und/oder seinen Tochterunternehmen in den USA oder in anderen Ländern. iOS wird unter Lizenz von Apple Inc. verwendet.

© 2013 BlackBerry. Alle Rechte vorbehalten. BlackBerry®, BBM™ und die zugehörigen Marken, Namen und Logos sind Eigentum von BlackBerry Limited und sind in den USA und/oder weiteren Ländern weltweit als Marken eingetragen und/oder werden dort als Marken verwendet. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

BlackBerry Technical Support Services Beim Einsatz von BES10 standardmäßig enthalten

Support ist eine strategische Schlüsselkomponente beim Enterprise Mobility Management. Die Implementierung von BES10 ist einfacher als jemals zuvor, dennoch ist ein starker Partner unverzichtbar, damit Sie Ihre Mobilitätsziele auch erreichen. Daher bieten Ihnen die BlackBerry Technical Support Services eine einzigartige Mischung aus technischer Expertise, schneller Problemlösung und proaktiver Unterstützung. Schließlich sollen Sie das volle Potenzial Ihrer plattformübergreifenden BES10 Management Infrastruktur nutzen.

Wenn Sie BES10 einsetzen, ist der BlackBerry Care Support bereits standardmäßig enthalten. So profitieren Sie vom elektronischen Zugriff auf BlackBerry Experten für zwei namentlich benannte Kontakte, von der garantierten Antwortzeit am nächsten Geschäftstag, von hilfreichen Schulungen und von zahlreichen Tools für mehr Produktivität und zur Fehlerdiagnose. Sie können sich aber auch umfassenderen Support sichern. Denn so bekommen Sie genau die technische Expertise, Unterstützung, Antwort- und Lösungszeiten, die Ihr Unternehmen braucht.

Weitere Informationen hierzu finden Sie unter blackberry.com/btss.