



BlackBerry UEM Client per iOS

Manuale dell'utente

Sommario

- Guida introduttiva a BlackBerry UEM Client..... 4**
 - Attivazione del dispositivo iOS.....4
 - Installazione o aggiornamento delle app di lavoro..... 6
 - Configurazione dell'account e-mail di lavoro..... 6
 - Utilizzo di BlackBerry UEM Self-Service..... 7
 - Uso di BlackBerry 2FA..... 7
 - Uso dell'autenticazione diretta.....7
 - Uso della password monouso.....7
 - Preautenticazione del dispositivo.....8

- Check out e check in nei dispositivi condivisi..... 9**

- Informazioni sulla conformità dei dispositivi..... 10**

- Informazioni sui criteri IT..... 11**

- Informazioni sui profili..... 12**

- Informazioni sui certificati..... 13**
 - Importazione dei certificati Entrust..... 13

- Dettagli sul menu Informazioni sulla privacy..... 14**

- Informazioni sulla valutazione e la recensione delle app..... 15**

- Modifica della password dell'app BlackBerry Dynamics..... 16**

- Caricare i file di registro in BlackBerry Support..... 17**

- Disattivazione del dispositivo..... 18**
 - Eliminazione di BlackBerry UEM Client..... 18

- Note legali..... 19**

Guida introduttiva a BlackBerry UEM Client

È possibile utilizzare BlackBerry UEM Client per attivare il dispositivo per il lavoro. Quando si attiva, il dispositivo viene associato a BlackBerry UEM e potrà accedere ai dati di lavoro e alle app per la produttività che l'amministratore ha assegnato al dispositivo stesso. L'amministratore determina il grado di protezione per il dispositivo in base al ruolo dell'utente e assegna profili e criteri IT per garantire che all'utente siano disponibili le funzioni del dispositivo appropriate oltre a proteggere i dati di lavoro in esso contenuti.

È possibile scaricare BlackBerry UEM Client per i dispositivi iOS da App Store.

Attivazione del dispositivo iOS

Il dispositivo è pronto per l'attivazione quando si riceve un messaggio e-mail di attivazione dall'amministratore.


Il messaggio e-mail di attivazione include le informazioni necessarie per attivare il dispositivo. Se la password di attivazione è già scaduta, creare una nuova password in BlackBerry UEM Self-Service oppure contattare l'amministratore.

Se si riceve un'attivazione QR Code tramite e-mail di attivazione, è possibile utilizzarla per attivare il dispositivo. Se si attiva un dispositivo con QR Code, non è necessario digitare alcuna informazione.

Se l'amministratore ha inviato istruzioni sull'uso delle credenziali aziendali, si verrà reindirizzati alla pagina di accesso dell'organizzazione per attivare il dispositivo.

Prima di iniziare: Se la modalità di blocco è attivata sul dispositivo (iOS e iPadOS 16 o versioni successive), è necessario disattivarla per attivare il dispositivo. La modalità di blocco impedisce l'installazione dei profili di configurazione richiesti per l'attivazione. Se necessario, è possibile abilitare la modalità di blocco dopo aver completato l'attivazione.

1. Installare BlackBerry UEM Client da App Store.
2. Aprire UEM Client.
3. Leggere e accettare il contratto di licenza.
4. Effettuare una delle operazioni descritte di seguito:

Attività	Procedura
Uso di QR Code per attivare il dispositivo	<ol style="list-style-type: none">a. Toccare  Acquisisci codice QR.b. Analizzare il QR Code nel messaggio e-mail di attivazione.
Uso delle credenziali aziendali per attivare il dispositivo	<ol style="list-style-type: none">a. Toccare Accedere nell'account dell'organizzazione se indicato dall'amministratore.b. Immettere l'indirizzo e-mail di lavoro. Questo è l'indirizzo e-mail con cui si è ricevuta l'e-mail di attivazione. Toccare Avanti.c. Immettere il nome utente e toccare Avanti. Si verrà reindirizzati alla pagina di accesso dell'organizzazione.d. Accedere utilizzando le proprie credenziali.

Attività	Procedura
Attivazione manuale del dispositivo	<ol style="list-style-type: none"> a. Immettere l'indirizzo e-mail di lavoro. Questo è l'indirizzo e-mail con cui si è ricevuta l'e-mail di attivazione. Toccare Vai. b. Se necessario, immettere l'indirizzo server fornito nell'e-mail di attivazione e toccare Attiva il mio dispositivo. c. Immettere la password di attivazione e toccare Attiva il mio dispositivo. Se la password di attivazione è scaduta, creare una nuova password in BlackBerry UEM Self-Service oppure contattare l'amministratore.

5. Toccare **Consenti** per consentire a UEM Client di inviare notifiche. Se si sceglie **Non consentire**, il dispositivo non si attiva completamente.
6. Quando viene richiesto di installare un certificato, toccare **OK**.
7. Quando viene richiesto di scaricare il profilo di configurazione, toccare **Consenti**.
8. Al termine del download, aprire **Impostazioni**.
9. Toccare **Generale** e accedere a **Profili e gestione dispositivi**.
10. Per installare il profilo, toccare **Profilo UEM** e seguire le istruzioni visualizzate sullo schermo.
11. Al termine dell'installazione, tornare all'app BlackBerry UEM Client per completare l'attivazione.
12. Se l'amministratore ha configurato l'accesso condizionale Microsoft Azure, è possibile effettuare una delle seguenti operazioni:

Attività	Procedura
Installare l'app Microsoft Authenticator sul dispositivo e accedere a Microsoft Azure	<ol style="list-style-type: none"> a. Nella schermata di registrazione del dispositivo online Microsoft, toccare Continua. b. Accedere utilizzando le credenziali Microsoft Azure. c. Nella schermata Aiutaci a mantenere protetto il dispositivo, è necessario scaricare l'app Microsoft Authenticator. Toccare Scarica l'app. d. Nell'app store, toccare Installa. e. Quando richiesto di autorizzare la raccolta dei dati di diagnostica, toccare OK. f. Accedere utilizzando le credenziali Microsoft Azure. g. Toccare Registra.

Attività	Procedura
Accedere a Microsoft Azure	<ol style="list-style-type: none"> Nella schermata di registrazione del dispositivo online Microsoft, toccare Continua. Toccare il proprio account. Accedere utilizzando le credenziali Microsoft Azure. Nella schermata Aiutaci a mantenere protetto il dispositivo, toccare Registra. Toccare Apri per visualizzare la schermata di conformità UEM Client.

13. Se richiesto, seguire le istruzioni visualizzate sullo schermo per installare le app di lavoro sul dispositivo.

Al termine: Per verificare che il processo di attivazione sia stato completato correttamente, effettuare una delle azioni seguenti:

- In UEM Client, toccare **Informazioni**. Nella sezione **Dispositivo attivato**, verificare che siano presenti le informazioni sul dispositivo e l'indicatore data/ora di attivazione.
- Nella console BlackBerry UEM Self-Service, verificare che il dispositivo sia indicato come dispositivo attivato. L'aggiornamento dello stato può richiedere fino a due minuti in seguito all'attivazione del dispositivo.

Installazione o aggiornamento delle app di lavoro

Se un'app richiesta non è installata, l'amministratore può limitare o rimuovere l'accesso ai dati di lavoro. Le applicazioni opzionali sono applicazioni consigliate dall'amministratore ma che non devono necessariamente essere installate sul dispositivo.

Quando l'utente scarica una app richiesta o opzionale da utilizzare a fini di lavoro, potrebbe essere necessario pagare per l'app e successivamente richiedere il rimborso del costo all'organizzazione.

Prima di iniziare: [Attivazione del dispositivo](#)

1. Nell'app BlackBerry UEM Client, toccare **App di lavoro**. Se non è presente la scheda App di lavoro, andare nella schermata iniziale del dispositivo e aprire l'app **App di lavoro**.
2. Effettuare una delle operazioni descritte di seguito:
 - Per installare le app di lavoro, toccare la scheda **Richieste** e installare tutte le app richieste, quindi toccare la scheda **Tutte** e installare le app opzionali desiderate.
 - Per aggiornare le app di lavoro, toccare la scheda **Nuove** e **Aggiorna** accanto a ciascuna app che si desidera aggiornare.

Configurazione dell'account e-mail di lavoro

Dopo aver attivato il dispositivo, è possibile ricevere una notifica per la configurazione del proprio indirizzo e-mail di lavoro. Seguire le istruzioni visualizzate sullo schermo per completare la configurazione. Se l'indirizzo e-mail di lavoro non viene configurato automaticamente, contattare l'amministratore per ulteriori informazioni.

Utilizzo di BlackBerry UEM Self-Service

È possibile utilizzare la console BlackBerry UEM Self-Service per impostare le password di attivazione, gestire le app BlackBerry Dynamics, preautenticare i dispositivi ed eseguire comandi di base come bloccare un dispositivo o modificare una password del dispositivo. Per ulteriori informazioni sull'uso di BlackBerry UEM Self-Service, [vedere il Manuale dell'utente di BlackBerry UEM Self-Service](#).

Uso di BlackBerry 2FA

Se l'amministratore ha attivato BlackBerry 2FA sul dispositivo per l'autenticazione a due fattori, il dispositivo può essere utilizzato come secondo fattore di autenticazione. Ciò assicura l'accesso alle risorse dell'organizzazione solo agli utenti autorizzati. Ad esempio, dopo aver immesso la password della directory per accedere alle risorse, sul dispositivo viene subito richiesta la conferma della connessione.

Il primo fattore è la password della directory. Il secondo fattore può essere uno dei seguenti:

- Una richiesta sul dispositivo da confermare prima della scadenza.
- Una password monouso da immettere assieme al nome utente o alla password della directory.

Nella schermata iniziale di BlackBerry UEM Client, scorrere a sinistra o a destra per accedere alle funzioni BlackBerry 2FA attivate dall'amministratore.

Uso dell'autenticazione diretta

Se l'amministratore ha configurato BlackBerry 2FA per il dispositivo e ha attivato la funzione di autenticazione diretta per il dispositivo, è possibile autenticarsi preventivamente da BlackBerry UEM Client prima di accedere alle risorse dell'organizzazione. Quando si utilizza l'autenticazione diretta, è necessario utilizzare la password della directory per accedere alle risorse dell'organizzazione entro il limite di tempo specificato dall'amministratore. È anche possibile utilizzare la funzione di autenticazione diretta per autenticarsi per le risorse dell'organizzazione invece di ricevere una richiesta di conferma e senza utilizzare una password monouso.

1. Nella schermata iniziale di BlackBerry UEM Client, scorrere fino alla schermata **Autenticazione diretta**.
2. Toccare **Autentica ora**.
Viene visualizzato un messaggio una volta completata l'autenticazione.

Al termine: Accedere alle risorse dell'organizzazione utilizzando la password della directory entro il tempo specificato nella schermata **Autenticazione diretta**.

Uso della password monouso

Se un amministratore ha configurato BlackBerry 2FA per il dispositivo e ha attivato la funzione per la password monouso per il dispositivo, è possibile utilizzare la password monouso visualizzata su BlackBerry UEM Client quando si accede alle risorse dell'organizzazione. Immettere la password monouso assieme al nome utente e alla password della directory. È possibile utilizzare una password monouso quando il dispositivo non può ricevere richieste di conferma per mancanza di sufficiente connettività di rete.

1. Nella schermata iniziale di BlackBerry UEM Client, scorrere fino alla schermata **Password monouso**.
2. Prendere nota della password monouso. Tutte le password monouso scadono dopo 30 secondi.
3. Sul computer o dispositivo da cui si sta tentando di accedere alle risorse dell'organizzazione, effettuare una delle seguenti operazioni:
 - Nel campo **Nome utente**, immettere il nome utente, una virgola (,) e la password monouso. Nome utente e password monouso sono separati solo da una virgola (senza spazi). Ad esempio, se il nome utente è "janedoe" e la password monouso è "555123", digitare "janedoe,555123".

- Nel campo **Password**, immettere la password monouso prima della password della directory (senza spazi o caratteri di separazione). Ad esempio, se la password monouso è "123456" e la password della directory è "qweRTY", digitare "123456qweRTY".

Preautenticazione del dispositivo

Se l'amministratore ha configurato BlackBerry 2FA per il dispositivo, è possibile richiedere la preautenticazione da BlackBerry UEM Client. La preautenticazione consente di accedere alle risorse di lavoro per un determinato periodo di tempo senza che venga richiesta la conferma o una password sul dispositivo. È possibile utilizzare la funzione di preautenticazione quando si è certi di non avere accesso al dispositivo, di trovarsi in un'area senza copertura mobile oppure di poter connettere solo un dispositivo a una rete wireless o a un hotspot. Ad esempio, se è possibile connettere a una rete un solo dispositivo alla volta, è possibile preautenticarsi sul dispositivo mobile in uso e quindi accedere alle risorse di lavoro dall'altro dispositivo.

È anche possibile eseguire la preautenticazione del dispositivo dalla console BlackBerry UEM Self-Service. Per ulteriori informazioni sull'uso di BlackBerry UEM Self-Service, [vedere il Manuale dell'utente di BlackBerry UEM Self-Service](#).

1. Nella schermata iniziale di BlackBerry UEM Client, scorrere fino alla schermata **Preautenticazione**.
2. Toccare **Richiedi preautenticazione**.
3. Immettere il numero di ore per le quali si desidera ricevere la preautenticazione. L'amministratore specifica il numero massimo di ore per le quali si può ricevere la preautenticazione.
4. Toccare **Richiedi**.
Viene visualizzata una schermata di conferma della data e dell'ora di scadenza della preautenticazione.
5. Toccare **Chiudi**.

Check out e check in nei dispositivi condivisi

Se l'amministratore assegna all'utente un dispositivo che verrà condiviso con altri utenti, è necessario eseguire il check out del dispositivo da utilizzare. Una volta terminato l'uso del dispositivo, è possibile eseguire il check in affinché il dispositivo sia disponibile per gli altri utenti.

1. Aprire UEM Client.
2. Se necessario, leggere e accettare le condizioni per l'utilizzo del servizio.
3. Effettuare una delle attività descritte di seguito:

Attività	Procedura
Eseguire il check out di un dispositivo.	<ol style="list-style-type: none">a. Per modificare l'opzione di autenticazione, toccare l'elenco a discesa e procedere come segue:<ol style="list-style-type: none">1. Nell'elenco a discesa, selezionare Microsoft Active Directory o Autenticazione diretta.2. Toccare Fine.b. Se si seleziona Microsoft Active Directory, digitare il dominio dell'organizzazione.c. Digitare il nome utente e la password.d. Toccare Check Out.e. Toccare OK.
Eseguire il check in di un dispositivo.	<ol style="list-style-type: none">a. Toccare Check In.b. Toccare OK.

Informazioni sulla conformità dei dispositivi

È possibile toccare lo stato di conformità nella schermata iniziale di BlackBerry UEM Client per visualizzare il report di conformità. Il report sulla conformità elenca i criteri applicati dall'organizzazione al dispositivo.

Se il dispositivo non è conforme e il problema di conformità non viene risolto prima della data visualizzata nel rapporto di conformità, l'amministratore può limitare o bloccare l'accesso del dispositivo alle risorse e alle reti di lavoro. Se non si è in grado di risolvere il problema, contattare l'amministratore.

Di seguito sono riportati alcuni criteri di conformità che l'organizzazione può applicare:

- **Stato rooted o jailbroken:** se il dispositivo è rooted, l'utente o qualcun altro ha eseguito un software o effettuato un'operazione sul dispositivo che consente l'accesso root al sistema operativo del dispositivo. L'utente o l'amministratore potrebbero dover rimuovere il software di rooting dal dispositivo oppure effettuare alcune operazioni sul dispositivo per ripristinare lo stato predefinito del dispositivo.
- **Password:** la password sul dispositivo deve soddisfare i requisiti di complessità specificati dall'organizzazione.
- **Modello dispositivo:** l'organizzazione potrebbe consentire l'attivazione per lavoro solo di determinati modelli di dispositivo. È necessario utilizzare un dispositivo che soddisfi i requisiti di sicurezza dell'organizzazione.
- **Versione OS:** l'organizzazione potrebbe consentire l'attivazione per lavoro solo dei dispositivi sui quali sono in esecuzione determinate versioni di Android OS.
- **Livello patch di sicurezza:** le patch di sicurezza vengono distribuite dal produttore del dispositivo e possono essere trovate quando si verifica la presenza di aggiornamenti del sistema sul dispositivo. Installare la patch di sicurezza più recente disponibile per il modello di dispositivo.
- **Dispositivo fuori contatto:** un dispositivo è fuori contatto se BlackBerry UEM non è in grado di contattarlo dopo un intervallo di tempo specifico. Ad esempio, il dispositivo potrebbe essere fuori contatto se non ha una connessione di rete.
- **App di lavoro richieste installate:** le app richieste che l'organizzazione intende installare sul dispositivo vengono visualizzate nella schermata App di lavoro assegnate. L'amministratore è in grado di stabilire se le app richieste non sono installate e, in questo caso, limitare l'accesso ai dati di lavoro. Se per un'app di lavoro è disponibile un aggiornamento, è necessario installarlo sul dispositivo.
- **App non assegnate o con restrizioni installate:** se sul dispositivo è stata installata un'app che non è richiesta oppure opzionale assegnata che non viene assegnata per fini di lavoro, è necessario rimuovere l'app dal dispositivo. Tutte le app con restrizioni dovranno essere rimosse dal dispositivo.

Informazioni sui criteri IT

Un criterio IT è composto da una serie di regole che controllano le funzioni di protezione e il comportamento del dispositivo. Ad esempio, se l'organizzazione richiede che l'utente imposti una password per il dispositivo, l'amministratore applica al dispositivo un criterio IT che include una regola che richiede l'impostazione di una password da parte dell'utente. Nella schermata iniziale, toccare l'icona dei criteri IT per visualizzare le regole applicate al dispositivo.

Non è possibile modificare o disattivare una regola dei criteri IT. Le regole dei criteri IT applicate al dispositivo fanno parte dei criteri di protezione globali dell'organizzazione. Per ulteriori informazioni, contattare l'amministratore.

Informazioni sui profili

I profili consentono di accedere alle risorse di lavoro sul dispositivo. Ad esempio, l'amministratore assegna i profili all'account utente per consentire all'utente di accedere al proprio account e-mail di lavoro, alle connessioni Wi-Fi, alle connessioni VPN e ai certificati di protezione.

Nella schermata iniziale, è possibile toccare la sezione Profili assegnati per visualizzare i profili assegnati al dispositivo. Si noti che vengono visualizzati solo i profili applicabili a BlackBerry UEM Client.

Informazioni sui certificati

I certificati vengono utilizzati per autenticare l'accesso del dispositivo alle reti e alle risorse di lavoro.

Se l'amministratore assegna il profilo di un certificato all'account utente, si riceverà un messaggio sul dispositivo che richiede di installare il certificato. Registrare le informazioni visualizzate nel messaggio e seguire le istruzioni per l'installazione del certificato. Se viene richiesto di immettere una password non fornita in precedenza, contattare l'amministratore.

Importazione dei certificati Entrust

Se l'amministratore ha assegnato Entrust credenziali smart all'utente, l'utente deve attivarle dal portale self-service Entrust IdentityGuard e importare quindi i certificati nella schermata Profili in BlackBerry UEM Client.

Prima di iniziare:

- Attivare il dispositivo con BlackBerry UEM Client.
1. Accedere al portale self-service Entrust IdentityGuard .
 2. Ottenere il QR Code e la password dal portale self-service Entrust IdentityGuard.
 - a) Fare clic su **Desidero attivare o aggiornare le mie credenziali smart**.
 - b) Selezionare nuovamente l'opzione **Desidero attivare o aggiornare le mie credenziali smart**. Fare clic su **Avanti**.
 - c) Selezionare una delle credenziali smart da utilizzare. Fare clic su **OK**.
 - d) Selezionare l'opzione **Sto attivando un'identità con credenziale smart mobile ospitata su un dispositivo mobile**. Fare clic su **Avanti**.
 - e) Selezionare l'opzione **Attiva la mia credenziale smart facendo utilizzare al mio dispositivo la rete dati ad essa associata**. . Fare clic su **Avanti**.
 - f) Nel campo **Nome identità**, digitare un nome. Fare clic su **OK**.
Viene visualizzato il QR Code e una password.
 3. Sul dispositivo, aprire° UEM Client.
 4. Toccare **Profili > Importa certificati**.
 5. Accanto alle credenziali smart Entrust , toccare **Attiva**.
 6. Toccare l'icona della fotocamera e acquisire QR Code dal portale self-service Entrust IdentityGuard.
 7. Immettere la password dal portale self-service Entrust IdentityGuard. Fare clic su **OK**.
Viene visualizzato un messaggio "Attivazione in corso. Attendere.". Questa operazione può richiedere alcuni minuti.
 8. Viene visualizzato un messaggio di conferma dell'avvenuta operazione. Fare clic su **OK**.

Dettagli sul menu Informazioni sulla privacy

Il menu Informazioni sulla privacy consente di visualizzare le informazioni visibili e non visibili dall'amministratore IT. Il menu elenca anche le azioni che l'amministratore può e non può eseguire sul dispositivo.

Nota: Il menu Informazioni sulla privacy è disponibile per tutti i tipi di attivazioni, ad eccezione delle attivazioni BlackBerry 2FA.



Nota: Il menu Informazioni sulla privacy è disponibile solo se il dispositivo è stato attivato per BlackBerry UEM versione 12.11.

Informazioni sulla valutazione e la recensione delle app

L'amministratore può consentire agli utenti di valutare le app e vedere le recensioni scritte da altri utenti. È possibile valutare un'app senza scrivere una recensione, ma se si scrive una recensione è necessario includere una valutazione. Dopo aver valutato e scritto una recensione su un'app, è possibile modificare o eliminare la valutazione e la recensione.



Modifica della password dell'app BlackBerry Dynamics

Se l'amministratore consente a BlackBerry UEM Client di autenticare altre app BlackBerry Dynamics, è possibile modificare la password dell'app BlackBerry Dynamics in BlackBerry UEM Client. È possibile utilizzare la password dell'app BlackBerry Dynamics per attivare e accedere alle app protette da BlackBerry Dynamics.

1. Nella schermata iniziale di BlackBerry UEM Client, toccare .
2. Toccare .
3. Toccare **Informazioni**.
4. Toccare **Password app BlackBerry Dynamics**.
5. Immettere la password corrente.
6. Immettere e confermare la nuova password.
7. Toccare **OK**.

Caricare i file di registro in BlackBerry Support

Se richiesto da BlackBerry Support, è possibile caricare i file di registro per risolvere un problema relativo alle app BlackBerry Dynamics.

1. Toccare  per aprire BlackBerry Dynamics Launcher.
2. Toccare .
3. Nella sezione **Supporto**, fare clic su **Carica registri**. La barra di stato del caricamento dei registro mostra l'avanzamento dell'operazione.
4. Fare clic su **Chiudi**.

Disattivazione del dispositivo

Se non si desidera che l'amministratore gestisca il dispositivo, è possibile disattivarlo. Se il dispositivo viene disattivato, la connessione tra il dispositivo e le risorse di lavoro viene rimossa. Una volta disattivato il dispositivo, non è possibile connettersi all'account e-mail o al calendario di lavoro e non è possibile accedere alla connessione Wi-Fi o alla connessione VPN di lavoro.

Prima di iniziare: Assicurarsi che il dispositivo sia connesso alla rete wireless.

1. Nella schermata iniziale di BlackBerry UEM Client, toccare **Informazioni**.
2. Toccare **Disattiva**.
3. Toccare **OK**.

Al termine: [Eliminazione di BlackBerry UEM Client](#)

Eliminazione di BlackBerry UEM Client

Se si elimina BlackBerry UEM Client dal dispositivo, non è possibile attivare il dispositivo.

Prima di iniziare: Disattivare il dispositivo.

1. Toccare e tenere premuta l'icona **BlackBerry UEM Client**.
2. Toccare la **x** nella parte superiore dell'icona.
3. Toccare **Elimina**.

Al termine: Se si desidera attivare il dispositivo, reinstallare BlackBerry UEM Client sul dispositivo. È necessaria una nuova password di attivazione. Utilizzare BlackBerry UEM Self-Service per creare una password di attivazione oppure contattare l'amministratore.

Note legali

©2017 BlackBerry Limited. I marchi, tra cui BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU e SECUSMART sono marchi o marchi registrati di BlackBerry Limited, delle società sussidiarie e/o affiliate, concessi in licenza e i diritti esclusivi su tali marchi sono espressamente riservati. Tutti gli altri marchi sono di proprietà dei rispettivi titolari.

App Store è un marchio di Apple Inc. iOS è un marchio di Cisco Systems, Inc. e/o delle sue affiliate negli Stati Uniti e in altri Paesi. iOS® viene utilizzato con licenza di Apple Inc. Wi-Fi è un marchio di Wi-Fi Alliance. Tutti gli altri marchi sono di proprietà dei rispettivi titolari.

La presente documentazione, compresa tutta la documentazione ivi allegata come riferimento, ad esempio la documentazione fornita o resa disponibile sul sito Web di BlackBerry, viene fornita o resa accessibile "COSÌ COM'È" e "SE DISPONIBILE" e senza alcuna condizione, approvazione, garanzia o dichiarazione di alcun tipo da parte di BlackBerry Limited e delle relative società affiliate ("BlackBerry") e BlackBerry non si assume alcuna responsabilità per errori tipografici, tecnici o per altre imprecisioni, errori od omissioni presenti nella documentazione. Al fine di tutelare le informazioni proprietarie e confidenziali e/o i segreti commerciali di BlackBerry, è possibile che alcuni aspetti delle tecnologie di BlackBerry vengano descritti in modo generico nella presente documentazione. BlackBerry si riserva il diritto di modificare periodicamente le informazioni contenute nella presente documentazione, senza alcun obbligo di distribuzione agli abbonati di modifiche, aggiornamenti, miglioramenti o aggiunte al documento in tempo utile.

La presente documentazione potrebbe contenere riferimenti a fonti di informazioni, hardware o software, prodotti o servizi di terzi, compresi componenti e contenuti protetti da copyright e/o siti Web di terzi (collettivamente denominati "Prodotti e servizi di terzi"). BlackBerry non controlla né è responsabile per eventuali Prodotti e servizi di terzi, inclusi, a titolo esemplificativo e non esaustivo, il contenuto, l'accuratezza, la conformità al copyright, le prestazioni, la compatibilità, l'affidabilità, la legalità, la decenza, i collegamenti o qualsiasi altro aspetto dei Prodotti e servizi di terzi. La presenza di riferimenti a Prodotti e servizi di terzi nella presente documentazione non implica in alcun caso l'approvazione da parte di BlackBerry dei Prodotti e servizi di terzi o dei terzi.

FATTA ECCEZIONE PER QUANTO ESPRESSAMENTE PROIBITO DALLE LEGGI APPLICABILI NELLA GIURISDIZIONE VIGENTE, CON IL PRESENTE DOCUMENTO SI ESCLUDONO TUTTE LE CONDIZIONI, APPROVAZIONI, GARANZIE, DICHIARAZIONI IMPLICITE O ESPLICITE DI OGNI GENERE, COMPRESSE, SENZA ALCUNA LIMITAZIONE, LE CONDIZIONI, APPROVAZIONI, GARANZIE, DICHIARAZIONI O GARANZIE DI DURATA, IDONEITÀ A UN PARTICOLARE SCOPO O USO, COMMERCIALIZZABILITÀ, QUALITÀ, NON VIOLAZIONE, QUALITÀ SODDISFACENTE O TITOLO, OPPURE DERIVANTI DA STATUTI O USANZE COMMERCIALI O USI DI COMMERCIO O ANCORA CORRELATE ALLA DOCUMENTAZIONE O ALL'USO DI QUESTA, O ALLE PRESTAZIONI O ALLE MANCATE PRESTAZIONI DI SOFTWARE, HARDWARE, SERVIZI O QUALSIASI TIPO DI PRODOTTI E SERVIZI DI TERZI IVI NOMINATI. L'UTENTE POTREBBE INOLTRE GODERE DI ULTERIORI DIRITTI A SECONDA DELLO STATO O DELLA PROVINCIA DI APPARTENENZA. È POSSIBILE CHE ALCUNE GIURISDIZIONI NON CONSENTANO L'ESCLUSIONE O LA LIMITAZIONE DI GARANZIE E CONDIZIONI IMPLICITE. NEI LIMITI CONSENTITI DALLA LEGGE, TUTTE LE GARANZIE E CONDIZIONI IMPLICITE IN RELAZIONE ALLA PRESENTE DOCUMENTAZIONE, QUALORA LA LORO ESCLUSIONE NON FOSSE CONCESSA, IN BASE A QUANTO SPECIFICATO SOPRA, MENTRE NE RISULTA CONCESSA LA LIMITAZIONE, VENGONO QUI LIMITATE A NOVANTA (90) GIORNI A PARTIRE DALLA DATA DI ACQUISIZIONE DELLA DOCUMENTAZIONE O DELL'ARTICOLO OGGETTO DI RECLAMO.

ENTRO I LIMITI MASSIMI CONSENTITI DALLE LEGGI APPLICABILI NELLA GIURISDIZIONE VIGENTE, BLACKBERRY NON PUÒ ESSERE IN NESSUN CASO RITENUTA RESPONSABILE DI QUALSIASI TIPO DI DANNI RELATIVI ALLA PRESENTE DOCUMENTAZIONE O ALL'USO DI QUESTA, OVVERO ALLE PRESTAZIONI O MANCATE PRESTAZIONI DI QUALSIASI SOFTWARE, HARDWARE, SERVIZIO O QUALSIASI DEI PRODOTTI E SERVIZI DI TERZI DI CUI SOPRA, COMPRESI, SENZA LIMITAZIONE, I DANNI SEGUENTI: DIRETTI, CONSEGUENZIALI, ESEMPLARI, INCIDENTALI, INDIRETTI, SPECIALI, PUNITIVI O AGGRAVATI, DANNI DERIVANTI DALLA PERDITA DI RICAVI O PROFITTI, MANCATA REALIZZAZIONE DEI GUADAGNI PREVISTI, INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, PERDITA DI INFORMAZIONI COMMERCIALI, PERDITA DI OPPORTUNITÀ COMMERCIALI OVVERO DANNEGGIAMENTO O PERDITA DI DATI, MANCATA TRASMISSIONE O RICEZIONE DI DATI, PROBLEMI ASSOCIATI A QUALSIASI DELLE

APPLICAZIONI UTILIZZATE CON I PRODOTTI O I SERVIZI BLACKBERRY, COSTI DERIVANTI DA TEMPI MORTI, MANCATO USO DEI PRODOTTI O DEI SERVIZI BLACKBERRY O DI PARTI DI ESSI OVVERO DI QUALSIASI SERVIZIO DI DISPONIBILITÀ, COSTO DI SERVIZI SOSTITUTIVI, COSTI DI COPERTURA, STRUTTURE O SERVIZI, COSTI DI CAPITALE OVVERO ALTRE PERDITE DI CARATTERE PECUNIARIO DI TALE TIPO, SIA NEL CASO IN CUI TALI DANNI SIANO PREVISTI CHE NEL CASO IN CUI NON LO SIANO, E ANCHE QUALORA BLACKBERRY SIA STATA AVVISATA DELLA POSSIBILITÀ DEL VERIFICARSI DI TALI DANNI.

ENTRO I LIMITI MASSIMI CONSENTITI DALLE LEGGI APPLICABILI NELLA GIURISDIZIONE VIGENTE, BLACKBERRY NON HA NESSUN ALTRO TIPO DI OBBLIGO, DOVERE O RESPONSABILITÀ RELATIVAMENTE AD ADEMPIMENTO DEL CONTRATTO, NEGLIGENZA O ALTRO NEI CONFRONTI DELL'UTENTE, INCLUSE LA RESPONSABILITÀ PER NEGLIGENZA E LA RESPONSABILITÀ OGGETTIVA.

LE LIMITAZIONI, ESCLUSIONI ED ESCLUSIONI DI RESPONSABILITÀ RIPORTATE NEL PRESENTE DOCUMENTO SI APPLICANO: (A) INDIPENDENTEMENTE DALLA NATURA DELLA CAUSA DELL'AZIONE, DELLA RICHIESTA O DELL'AZIONE INTRAPRESA DALL'UTENTE, COMPRESSE, SENZA LIMITAZIONE, LA VIOLAZIONE DEL CONTRATTO, LA NEGLIGENZA, LE AZIONI LESIVE, LA COMPATIBILITÀ O QUALSIASI ALTRO DANNO CONTEMPLATO DALLA LEGGE E RIMARRANNO IN VIGORE IN SEGUITO A VIOLAZIONI DI FONDO O AL MANCATO ADEMPIMENTO DELLO SCOPO ALLA BASE DEL PRESENTE CONTRATTO O DI QUALSIASI CLAUSOLA IN ESSO PRESENTE; E (B) A BLACKBERRY E ALLE RELATIVE SOCIETÀ AFFILIATE, AI SUCCESSORI DI QUESTE, AI CESSIONARI, AGLI AGENTI, AI FORNITORI (IVI COMPRESI I PROVIDER DI SERVIZI), AI RIVENDITORI AUTORIZZATI BLACKBERRY (IVI COMPRESI I PROVIDER DI SERVIZI) E AI RISPETTIVI DIRETTORI, DIPENDENTI E COLLABORATORI INDIPENDENTI.

OLTRE ALLE LIMITAZIONI ED ESCLUSIONI DI CUI SOPRA, IN NESSUN CASO SU DIRETTORI, DIPENDENTI, AGENTI, DISTRIBUTORI, FORNITORI, COLLABORATORI INDIPENDENTI DI BLACKBERRY O SU QUALSIASI AFFILIATO DI BLACKBERRY RICADRÀ LA RESPONSABILITÀ DERIVANTE DA O CORRELATA ALLA PRESENTE DOCUMENTAZIONE.

Prima della sottoscrizione, dell'installazione o dell'utilizzo di Prodotti e servizi di terzi, è responsabilità dell'utente assicurarsi che il provider di servizi garantisca il supporto di tutte le relative funzioni. Alcuni provider di servizi di traffico telefonico potrebbero non offrire funzionalità di esplorazione in Internet con un abbonamento a BlackBerry® Internet Service. Verificare con il provider di servizi la disponibilità, gli accordi di roaming, i piani di servizi e le funzionalità. L'installazione o l'utilizzo di Prodotti e servizi di terzi con prodotti e servizi BlackBerry potrebbero richiedere uno o più brevetti, marchi, copyright o licenze di altro tipo al fine di evitare violazioni dei diritti di terzi. L'utilizzo di Prodotti e servizi di terzi e la verifica dell'eventuale necessità di disporre di licenze di terzi sono responsabilità esclusiva dell'utente. Qualora necessario, l'utente è responsabile della relativa acquisizione. L'utente non deve installare o utilizzare Prodotti e servizi di terzi prima dell'acquisizione delle licenze eventualmente necessarie. Tutti i Prodotti e servizi di terzi forniti con i prodotti e i servizi BlackBerry hanno lo scopo di offrire maggiore comodità all'utente e vengono forniti "COME SONO", senza condizioni, approvazioni, garanzie, dichiarazioni espresse o implicite di qualsiasi tipo da parte di BlackBerry. BlackBerry non si assume alcun tipo di responsabilità in merito. L'utilizzo da parte dell'utente di Prodotti e servizi di terzi deve essere sottoposto e soggetto all'accettazione da parte dell'utente stesso dei termini di licenze e altri contratti ivi applicabili con terzi, salvo quanto espressamente indicato da eventuali licenze o altri contratti stipulati con BlackBerry.

I termini di utilizzo di tutti i prodotti e servizi BlackBerry vengono definiti in una licenza a parte o in un altro contratto stipulato con BlackBerry ivi applicabile. NESSUNA AFFERMAZIONE CONTENUTA NELLA PRESENTE DOCUMENTAZIONE PUÒ SOSTITUIRE CONTRATTI O GARANZIE SCRITTI ESPlicitI FORNITI DA BLACKBERRY PER PARTI DI PRODOTTO O SERVIZI BLACKBERRY DIVERSI DA QUELLI INDICATI NELLA PRESENTE DOCUMENTAZIONE.

BlackBerry Enterprise Software include software di terze parti. La licenza e le informazioni sul copyright associate a tale software sono disponibili all'indirizzo <http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp>.

BlackBerry Limited
2200 University Avenue East

Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada