



BlackBerry UEM Client per Android

Manuale dell'utente

Sommario

| | |
|---|-----------|
| Guida introduttiva a BlackBerry UEM Client..... | 5 |
| Attivazione del dispositivo Android..... | 5 |
| Configurazione dell'autenticazione tramite impronta digitale..... | 7 |
| Installazione o aggiornamento delle app di lavoro..... | 7 |
| Configurazione dell'account e-mail di lavoro..... | 8 |
| Utilizzo di BlackBerry UEM Self-Service..... | 8 |
| Uso di BlackBerry 2FA..... | 8 |
| Uso dell'autenticazione diretta..... | 8 |
| Uso della password monouso..... | 9 |
| Preautenticazione del dispositivo..... | 9 |
| Informazioni sui tipi di attivazione..... | 10 |
| Informazioni sulla conformità dei dispositivi..... | 11 |
| Informazioni sui criteri IT..... | 12 |
| Informazioni sui profili..... | 13 |
| Informazioni sui certificati..... | 14 |
| Importazione dei certificati Entrust..... | 14 |
| Informazioni sulla privacy..... | 15 |
| Informazioni sulla valutazione e la recensione delle app..... | 16 |
| Modifica della password dell'app BlackBerry Dynamics..... | 17 |
| Caricare i file di registro in BlackBerry Support..... | 18 |
| Uso di un provider di identità di terze parti per sbloccare, attivare e ripristinare la propria password per le app BlackBerry Dynamics..... | 19 |
| Sblocco di un'app BlackBerry Dynamics utilizzando un provider di identità di terze parti..... | 19 |
| Attivazione di un'app BlackBerry Dynamics in seguito al ripristino del dispositivo utilizzando un provider di identità di terze parti..... | 19 |
| Ripristinare la password dell'app BlackBerry Dynamics utilizzando un provider di identità di terze parti..... | 20 |

Disattivazione del dispositivo.....21
 Eliminazione di BlackBerry UEM Client..... 21

Legal notice..... 22

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 Android da Google Play Store.

Attivazione del dispositivo Android

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 è necessaria una nuova e-mail di attivazione o la password di attivazione è già scaduta, creare una password in BlackBerry UEM Self-Service oppure contattare l'amministratore.

Se è stata ricevuta un'attivazione QR Code dall'amministratore, 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.

Per attivare il dispositivo, è necessario consentire a UEM Client di accedere alla fotocamera del dispositivo.

1. Sul dispositivo, installare BlackBerry UEM Client da Google Play.
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. Toccare Consenti per consentire a UEM Client di scattare foto e registrare video.c. Analizzare il QR Code nel messaggio e-mail di attivazione. |

| Attività | Procedura |
|-------------------------------------|---|
| Attivazione manuale del dispositivo | <ol style="list-style-type: none"> a. Toccare Immettere le credenziali fornite nell'e-mail. 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. Se necessario, immettere l'indirizzo server fornito nell'e-mail di attivazione e toccare Avanti. d. Se necessario, immettere il proprio nome utente. e. 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 effettuare e gestire le chiamate telefoniche.
6. Attendere che i profili e le impostazioni vengano inviati al dispositivo.
7. Nella schermata **Configura profilo**, toccare **Configura** e attendere mentre un profilo di lavoro viene impostato sul dispositivo.
8. Se viene richiesto, accedere al proprio account Google con indirizzo e-mail e password Google. Se non si ha un account Google, è possibile crearne uno ora.
9. Nella schermata di selezione dello sblocco, scegliere un metodo di sblocco dello schermo.
10. Se viene visualizzata la schermata **Avvio protetto**, toccare **Si** per richiedere una password all'avvio del dispositivo.
11. Immettere una password dispositivo e ripeterla per confermarla. Toccare **OK**.
12. Selezionare una delle opzioni per scegliere come visualizzare le notifiche. Toccare **Fine**.
13. Creare una password UEM Client e toccare **OK**. Se si utilizzano le app BlackBerry Dynamics, si utilizzerà anche questa password per accedere a tutte le app BlackBerry Dynamics.
14. Nella schermata successiva, toccare **Registrati** e seguire le istruzioni visualizzate sullo schermo se si desidera configurare l'autenticazione tramite impronte digitali per UEM Client e qualsiasi app BlackBerry Dynamics in uso. In caso contrario, toccare **Annulla**.
15. Se ci si è disconnessi dal dispositivo, sbloccare il dispositivo per completare l'attivazione di BlackBerry UEM.
16. Se richiesto, toccare **OK** per consentire la connessione a BlackBerry Secure Connect Plus e attendere mentre la connessione viene attivata.
17. Facoltativamente, se l'amministratore ha configurato l'accesso condizionale ad Microsoft Azure, effettuare una delle seguenti operazioni:

| Attività | Procedura |
|--|--|
| Installare l'app Microsoft Authenticator sul dispositivo e accedere a ad Microsoft Azure | <ol style="list-style-type: none"> Sulla schermata di registrazione del dispositivo online Microsoft, toccare Continua. Accedere con le credenziali di Microsoft Azure. Nella schermata Aiutaci a proteggere il tuo dispositivo, scaricare l'app Microsoft Authenticator. Toccare Scarica l'app. Nell'App Store toccare Installa. Quando richiesto di consentire la raccolta della diagnostica, toccare OK. Accedere con le credenziali di Microsoft Azure. Toccare Registra. |
| Accedere ad Microsoft Azure | <ol style="list-style-type: none"> Sulla schermata di registrazione del dispositivo online Microsoft, toccare Continua. Toccare l'account. Accedere con le credenziali di Microsoft Azure. Sulla schermata Aiutaci a proteggere il tuo dispositivo, toccare Registra. Toccare Apri per visualizzare la schermata della conformità con UEM Client. |

18. 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.

Configurazione dell'autenticazione tramite impronta digitale

Se l'amministratore consente l'uso di questa opzione e la funzione è supportata sul dispositivo, è possibile configurare l'autenticazione tramite impronta digitale per sbloccare BlackBerry UEM Client in sostituzione all'immissione della password. Se questa opzione non viene visualizzata, contattare l'amministratore.

1. Toccare .
2. Toccare .
3. Nella sezione Password e impronta digitale, toccare **Configura impronta digitale**.

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 assegnate**.
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**.

Informazioni sui tipi di attivazione

A seconda dei criteri dell'organizzazione, l'amministratore sceglierà un tipo di attivazione adatto al dispositivo. Alcuni tipi di attivazione consentono di utilizzare un solo profilo di lavoro sul dispositivo, mentre altri consentono di utilizzare un profilo di lavoro e un profilo personale. A seconda del tipo di attivazione, l'amministratore può gestire solo il profilo di lavoro oppure i profili di lavoro e personale. Se l'amministratore desidera gestire solo il profilo di lavoro, il profilo personale viene mantenuto privato. Ad esempio, se per il lavoro si utilizza un dispositivo personale, questo avrà un profilo personale e un profilo di lavoro. Se necessario, l'amministratore può eliminare i dati nel profilo di lavoro, ma non i dati nel profilo personale. Tuttavia, se si utilizza un dispositivo di lavoro di proprietà dell'organizzazione, l'amministratore può eliminare tutti i dati (nel profilo di lavoro e anche nel profilo personale) presenti sul dispositivo.

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 assegnati > 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**.

Informazioni sulla privacy

Prima di attivare il dispositivo, è possibile fare clic su un collegamento disponibile nel contratto di licenza per l'utente finale per visualizzare l'informativa sulla privacy di BlackBerry.

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 **Modifica password applicazione**.
4. Immettere la password corrente.
5. Immettere e confermare la nuova password.
6. 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. L'amministratore può abilitare la registrazione dettagliata delle app a livello di debug. Quando questa opzione è abilitata, i registri delle app possono aiutare a individuare le possibili cause dei problemi che gli utenti potrebbero riscontrare.

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**.

Uso di un provider di identità di terze parti per sbloccare, attivare e ripristinare la propria password per le app BlackBerry Dynamics

È possibile utilizzare le credenziali di accesso fornite dal provider di identità di terze parti dell'organizzazione per sbloccare, attivare e ripristinare la password per le app BlackBerry Dynamics.

Sblocco di un'app BlackBerry Dynamics utilizzando un provider di identità di terze parti

Se una delle app BlackBerry Dynamics, ad esempio BlackBerry Work, è stata bloccata, è possibile utilizzare il provider di identità dell'organizzazione per sbloccarla. Si noti che l'amministratore dell'organizzazione deve abilitare questa funzione prima di poterla utilizzare.

1. Nella schermata **Applicazione remota bloccata** del dispositivo, toccare **Sblocca**.
2. Nella schermata **Sblocco applicazione**, toccare **Accedi**.
3. Immettere l'indirizzo e-mail utilizzato per accedere al provider di identità della propria organizzazione e toccare **Avanti**.
4. Immettere il nome utente utilizzato per accedere al provider di identità della propria organizzazione e toccare **Avanti**.
5. Immettere la password utilizzata per accedere al provider di identità della propria organizzazione e toccare **Accedi**.
6. Una volta attivata l'app BlackBerry Dynamics, immettere e confermare una nuova password.

Attivazione di un'app BlackBerry Dynamics in seguito al ripristino del dispositivo utilizzando un provider di identità di terze parti

Dopo aver ripristinato il proprio dispositivo da un backup, è possibile accedervi con le credenziali fornite dal provider di identità di terze parti della propria organizzazione (ad esempio, Okta o Ping Identity) e attivare le app BlackBerry Dynamics.

1. Nella schermata **Sblocco applicazione**, toccare **Accedi**.
2. Immettere l'indirizzo e-mail utilizzato per accedere al provider di identità della propria organizzazione e toccare **Avanti**.
3. Immettere il nome utente utilizzato per accedere al provider di identità della propria organizzazione e toccare **Avanti**.
4. Immettere la password utilizzata per accedere al provider di identità della propria organizzazione e toccare **Accedi**.
5. Una volta attivata l'app BlackBerry Dynamics, immettere e confermare una nuova password.

Ripristinare la password dell'app BlackBerry Dynamics utilizzando un provider di identità di terze parti

Se la password per l'app BlackBerry Dynamics è stata dimenticata, è possibile utilizzare il provider di identità di terze parti della propria organizzazione per impostarne una nuova.

1. Una volta effettuato l'accesso all'app, nella schermata della password, toccare **Password dimenticata**.
2. Toccare **Accedi**.
3. Immettere l'indirizzo e-mail utilizzato per accedere al provider di identità della propria organizzazione e toccare **Avanti**.
4. Immettere il nome utente utilizzato per accedere al provider di identità della propria organizzazione e toccare **Avanti**.
5. Immettere la password utilizzata per accedere al provider di identità della propria organizzazione e toccare **Accedi**.
6. Una volta attivata l'app BlackBerry Dynamics, immettere e confermare una nuova password.

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: [Disattivazione del dispositivo](#)

1. Accedere a **Impostazioni > Applicazioni > Gestisci applicazioni** e toccare **UEM Client**.
2. Toccare **Disinstalla**.
3. Toccare **OK**.

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.

Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at <http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp>.

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

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

Published in Canada