



BlackBerry Persona

Product Overview

Contents

- What is BlackBerry Persona?..... 4**
 - Architecture: Persona Mobile..... 5
 - How does BlackBerry Persona determine a user's behavioral risk level?.....7
 - How does BlackBerry Persona determine a user's geozone risk level?..... 7
 - How does app anomaly detection work?.....8
- Configuring and using BlackBerry Persona..... 9**
- Workflow: Integrating Persona Mobile with BlackBerry Enterprise Identity..... 10**
- Use cases..... 11**
 - Adapting device behavior in a high-risk scenario.....11
 - Adapting device behavior in a low-risk scenario..... 11
 - Adapting device behavior in a defined geozone..... 12
 - Confirming a user's identity..... 12
- Legal notice..... 13**

What is BlackBerry Persona?

BlackBerry Persona is a cloud service that dynamically adapts the security requirements and behavior of your users' devices and work apps to their real-world contexts. For example, if a BlackBerry Dynamics app reports a location that is not typical for the user, Persona can dynamically limit the user's access to work apps, disable device features such as the camera, and enforce stricter authentication requirements. Likewise, if a BlackBerry Dynamics app reports a location that is typical for the user, Persona can apply device behaviors that make it easier to access work apps and resources.

Persona adds a layer of adaptive security to your organization's existing UEM domain without introducing an additional software footprint. It is a cloud service that collects data from existing BlackBerry solutions, including [BlackBerry Enterprise Identity](#) and BlackBerry Dynamics apps.

The Persona services gather and process behavioral data, app events, and location data to calculate risk levels for each user in real time:

- Behavioral risk: An assessment of risk based on the user's typical activities.
- Continuous authentication app anomaly risk: An assessment of risk based on a model of the user's typical BlackBerry Dynamics app usage. If an app reports behaviors or events that do not fit the user's model, Persona triggers an action that you configure (for example, a prompt for authentication or blocking apps).
- Geozone risk: An assessment of risk based on the user's proximity to learned locations. You can also define custom geozones with static risk levels (for example, a specific office location with a low risk level).

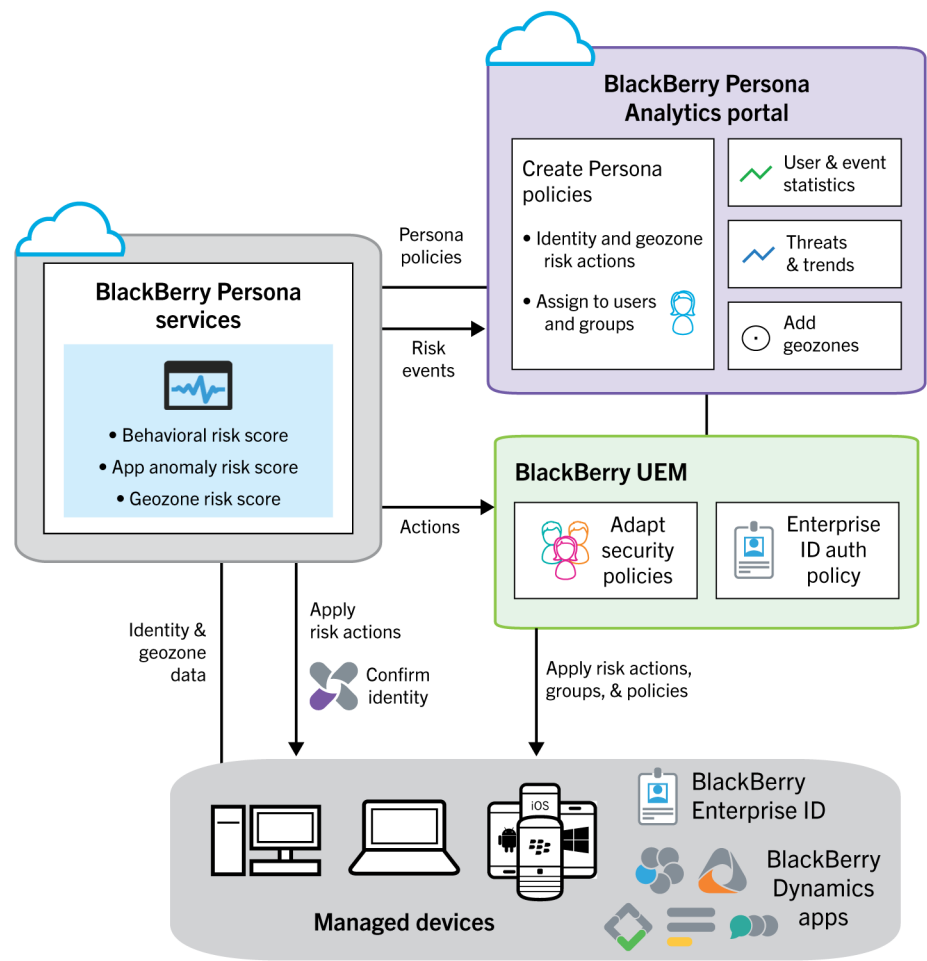
You can choose which risk engines you want Persona to use. For the different types and levels of risk, you can configure actions that you want Persona to execute when a user meets that risk criteria, including:

- Assigning the user to a local UEM group with policies, profiles, apps, and permissions appropriate for that risk level
- Assign a BlackBerry Dynamics profile that overrides the profile assigned in UEM
- Temporarily blocking all BlackBerry Dynamics apps
- Temporarily blocking the specific BlackBerry Dynamics app that initiated the risk assessment

After some initial configuration, Persona continuously applies adaptive and intelligent security standards to each user's device and work apps based on the user's behavior, device usage, and physical location, with no action required by users or administrators.

Persona also adds new functionality to BlackBerry Enterprise Identity authentication policies. You can now incorporate a user's behavioral risk level, geozone risk level, or a defined geozone into the factors that determine the authentication type required for work apps and services. For example, if a user's behavioral risk level is high, you can require the user to enter both a password and use BlackBerry 2FA to access work apps.

Architecture: Persona Mobile



Component	Description
Managed devices	<p>BlackBerry Enterprise Identity and BlackBerry Dynamics apps that use the BlackBerry Analytics SDK send usage data, events, and location data to the Persona services.</p> <p>The BlackBerry Dynamics apps released by BlackBerry (BlackBerry Work, BlackBerry Access, and so on) include the BlackBerry Analytics SDK.</p>

Component	Description
Persona services	<p>The Persona services receive usage data, events, and location data from BlackBerry Enterprise Identity and BlackBerry Dynamics apps. The services process this data and use machine learning to train and develop a risk model for each user.</p> <p>The services use this risk model to analyze new data that is received and to generate various risk scores for the user in real time, including a behavioral risk score, an app usage risk score, and a geozone risk score. The services communicate the user's current risk scores and the corresponding risk actions that you configure to BlackBerry Dynamics apps, the , and BlackBerry UEM.BlackBerry Persona Analytics Portal</p> <p>BlackBerry Dynamics apps support app anomaly risk detection. If the Persona services receive behavioral data or app events from BlackBerry Dynamics apps that do not fit the user's usage model, Persona triggers an authentication prompt. The user must successfully authenticate if they want to continue to use the app.</p>
BlackBerry Persona Analytics Portal	<p>You use the web-based BlackBerry Persona Analytics Portal to manage the service, including:</p> <ul style="list-style-type: none"> • Configuring and customizing the risk engines • Defining geozones to enforce security standards for specific locations • Creating and assigning Persona policies that apply adaptive actions to users' devices based on each user's level of risk • Viewing user and event statistics • Identifying trends and potential security threats <p>The portal communicates with the Persona services and UEM to apply policies to devices.</p>
BlackBerry UEM or BlackBerry UEM Cloud	<p>You use the UEM management console to create and configure local user groups that define security standards and device behaviors for the different risk levels and defined geozones. When you create a policy in the portal, you associate each group with one or more of the behavioral risk levels, geozone risk levels, or defined geozones.</p> <p>The Persona services communicate with UEM and direct it to apply risk actions (group assignments, temporary blocks of BlackBerry Dynamics apps) to users' devices.</p>
BlackBerry Enterprise Identity	<p>You can configure BlackBerry Enterprise Identity authentication policies that can change a user's authentication requirements in different risk scenarios. You can factor the user's behavioral risk level, geozone risk level, or a defined geozone into the risk factors in an authentication policy. If the user meets a certain risk level, the policy adapts the user's authentication requirements accordingly.</p>

How does BlackBerry Persona determine a user's behavioral risk level?

The Persona services calculate a user's behavioral risk level by processing the following contextual and behavioral data from BlackBerry Enterprise Identity and BlackBerry Dynamics apps:

- Geolocation (latitude/longitude)
- Unique user identifiers
- WAN IP
- BlackBerry Dynamics app identifiers
- Browser fingerprint (if using BlackBerry Enterprise Identity)

The majority of this data is provided by BlackBerry Dynamics apps.

The Persona services process this data and use machine learning to build a risk data model that characterizes a user's typical behavior. The data model is dynamic and is based on the user's last 30 days of activity. It can take some time to create a user's initial data model (for example, several days) because the services require a sufficient amount of user activity to establish a reliable model. The services retain user data for 30 days only (you can change the data retention period).

The Persona services assess incoming data based on the existing model and determine whether current data is consistent with the user's regular pattern of behavior and the behavior of similar device users in the organization (for example, for users in the same location). This assessment results in a risk level and corresponding risk actions for each user that are sent to UEM to execute.

The risk assessment can identify key security concerns, such as:

- Whether the user's current location is consistent with past behavior
- Whether the user's current location is possible based on the user's last reported location
- Whether and how often the device has accessed the current network
- Whether the user's app activity is consistent with past behavior

The services determine a user's risk level in real time as data is received. Geolocation data is given the most weight in the calculation of the risk level, followed by unique user identifier data, and then WAN IP and app identifier at equal weight. Browser fingerprint data is used as the app identifier for browser apps.

You can also enable a feature that allows users to reduce their behavioral risk level to low by completing a BlackBerry 2FA authentication prompt. This can help users avoid more restrictive group assignments when they engage in behaviors that do not fit their existing risk model (for example, the first time a user travels to a new office location or engages in different activities for a new role).

How does BlackBerry Persona determine a user's geozone risk level?

The Persona services process event and location data from apps to learn about the locations (geozones) that are typical for each user at different times. You can configure a Persona policy to execute risk actions based on the user's proximity to a learned geozone.

For example, if a user is in the range of a learned geozone at a given day and time, their geozone risk level is low and the assigned policy executes the actions for the low risk level. Likewise, if the user is out of the range of a learned geozone, their geozone risk level is medium or high (depending on how far out of range the user is) and the assigned policy executes the corresponding actions. You can customize the range for each geozone risk level.

The services can learn new geozones for a user over time. The first time that a user occupies a location that is outside of their typical geozones, their behavioral and geozone risk levels may be higher than usual, but if the user

is reported at that location with greater frequency, it can become a new learned geozone that results in a lower risk level.

You can use the BlackBerry Persona Analytics Portal to define specific geozones, each with a set risk level (high, medium, or low); you configure default risk actions for each risk level in a Persona policy. For example, you can define a geozone for a specific office location with a low risk level. If a user is in that geozone, their risk level will be low regardless of how far it is from their typical geozone. Note that the overall assessment of the user's geozone risk level is also impacted by the user's current behavioral risk assessment.

The Persona services retain user data for 30 days only (you can change the data retention period).

How does app anomaly detection work?

As a user uses the BlackBerry Dynamics apps, the apps send behavioral data and events to the Persona services, including the user's typical physical interactions with the app (scrolling, swiping, and so on) and frequently used device and app features (copy, screen shot, reply all, and so on).

The services use this information to train and develop a reliable usage model for the user based on established patterns of activity. The model is dynamic and based on the user's last 30 days of activity (you can change the data retention period). It can take some time to create a user's initial model as the services collect sufficient data.

If a BlackBerry Dynamics app reports behavior or app events that do not fit a user's established model, BlackBerry Persona immediately triggers an action that you specify in a policy. For example, you can apply a BlackBerry Dynamics override profile or block the app that the behavior was detected in.

This response to anomalous use is a direct and immediate way to protect users from malicious attempts to access valuable work data.

Configuring and using BlackBerry Persona

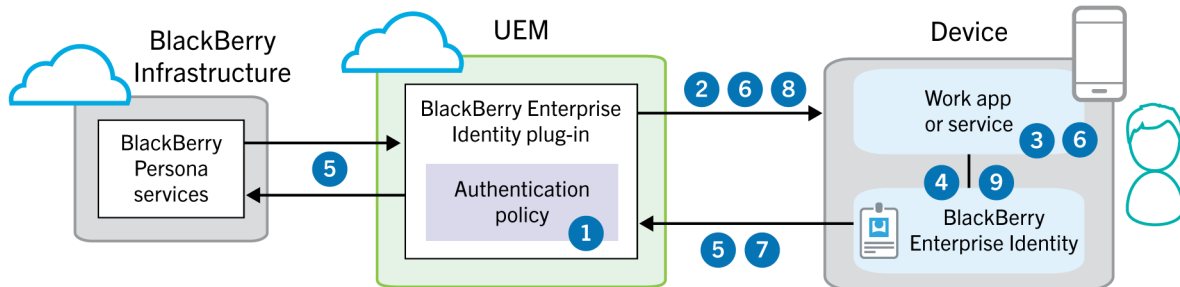
You complete the following steps to enable and use BlackBerry Persona in your organization's BlackBerry UEM or BlackBerry UEM Cloud domain. For software requirements and complete instructions for each step, see the [BlackBerry Persona Administration Guide](#).

1. Purchase BlackBerry Persona licenses for your organization's users. Assign the Persona entitlement to users.
2. Enable Persona in an existing or new UEM domain.
3. Assign a Persona administrator role to the users that will manage the service.
4. Optionally, customize the Persona risk engines and how long the service retains data.
5. Create local UEM user groups. Each group will be used for one or more of the behavioral risk levels, geozone risk levels, or defined geozones. Configure each group with a custom combination of IT policies, profiles, app assignments, and permissions that meet your organization's standards for each risk level or geozone.
6. Optionally, define geozones to set security standards for specific locations.
7. Create a Persona policy. The policy defines which risk engines you want Persona to use to determine user risk levels, and the actions the service should take for different types and levels of risk. How you configure the policy determines how Persona enforces adaptive security standards that are appropriate for each user's current activity and context.
8. Assign the Persona policy to users and groups.
9. Create and configure a BlackBerry Enterprise Identity authentication policy. When you add one or more risk scenarios that determine the authentication requirements for users, you can specify a behavioral risk level, a geozone risk level, or a defined geozone as a risk factor.
10. Assign the authentication policy to user groups. BlackBerry Enterprise Identity
11. By default, Persona runs in passive mode, where it collects data and builds risk models and learned locations for individual users, but does not execute risk actions. After enough data has been collected and used to create reliable risk models and learned locations, you can enable active mode.

BlackBerry Dynamics apps send app events and location data to the Persona services at regular intervals. BlackBerry Enterprise Identity sends data to the services at runtime. The services process this data to generate identity and geozone risk scores in real-time for each user. Based on your configuration of the policy, Persona executes management actions that correspond to a user's risk level (for example, assigning the user to a UEM group or temporarily blocking BlackBerry Dynamics apps).

Based on your configuration of the BlackBerry Enterprise Identity authentication policy, a user's current behavioral risk level, geozone risk level, or a defined geozone can also determine how the user logs in to services and work apps (for example, no authentication, single sign-on, password, BlackBerry 2FA, or a combination of methods).

Workflow: Integrating Persona Mobile with BlackBerry Enterprise Identity



This workflow describes how Persona can be integrated with BlackBerry Enterprise Identity to dynamically adapt a user's authentication requirements based on their current level of risk.

1. The administrator creates a Persona policy in the BlackBerry Persona Analytics Portal and a BlackBerry Enterprise Identity authentication policy in the UEM management console. The authentication policy specifies that if the user's behavioral risk level is high, the minimum authentication that is required is both a password and BlackBerry 2FA.
2. The administrator assigns the Persona policy and the authentication policy to a user account. The policies are applied to the user's device.
3. The user tries to log in to a work app or service on the device.
4. The app or service invokes BlackBerry Enterprise Identity for authentication.
5. BlackBerry Enterprise Identity determines the authentication policy that is assigned to the user and retrieves the user's current behavioral risk level from Persona.
6. If the user's behavioral risk level is high, the user is prompted for a password and BlackBerry 2FA authentication. The user enters their password and completes 2FA authentication.
7. BlackBerry Enterprise Identity sends the user credentials to UEM.
8. The BlackBerry Enterprise Identity plug-in authenticates the user and returns the user identity.
9. BlackBerry Enterprise Identity returns the successful authentication result and the user is logged in to the app or service.

Use cases

The following use cases demonstrate how you can use BlackBerry Persona in everyday situations. In the cases that follow, an administrator has configured and assigned a Persona policy and a BlackBerry Enterprise Identity authentication policy.

Adapting device behavior in a high-risk scenario

Jane Smith arrives at the airport for a business trip. She uses her work device, an iPhone, to access the airport's free Wi-Fi network.

The BlackBerry Dynamics apps on Jane's iPhone send data to the BlackBerry Persona services indicating that she is on a less secure network and that she is in a location that is far away from her typical learned location for that day and time. The services calculate a high behavioral risk level and a high geozone risk level and communicate these assessments to Jane's work apps, the , and UEM. The Persona policy that is applied to Jane's device takes effect, assigning Jane to a group with more restrictive device policies and profiles to ensure a higher level of security while Jane is at the airport.

When the new group configuration is applied to Jane's iPhone, she notices the following changes:

- When she tries to log in to work apps and services, she must provide both a UEM password and complete BlackBerry 2FA authentication.
- The iPhone camera is temporarily disabled.
- Bluetooth functionality is temporarily disabled.
- Her access to the company's intranet websites is currently restricted.
- Data synchronization to work apps, such as BlackBerry Work, occurs less frequently.

The new group assignment with these high-security device behaviors remains in place until Jane's behavioral and geozone risk level is recalculated and reduced. When she has a lower risk level, Persona will reassign her to a group that corresponds to the new risk level.

Adapting device behavior in a low-risk scenario

Bob Jones arrives at his company's main office to attend a lengthy board meeting. He checks his Android phone during the meeting to make sure that he doesn't miss any important emails. His phone is using the trusted, secure work network.

The BlackBerry Dynamics apps on Bob's Android device send data to the BlackBerry Persona services indicating that he is on a secure network and in a physical location that is typical for the current day and time. The services calculate a low behavioral risk level and geozone risk level and communicate these assessments to Bob's work apps, the BlackBerry Persona Analytics Portal, and UEM. The Persona policy that is applied to Bob's device takes effect and assigns Bob to a group with less restrictive device policies and profiles to ensure easy access to work resources in a highly secure location.

When the new group configuration is applied to Bob's phone, he notices the following changes:

- He can use fingerprint authentication to access work apps.
- He is prompted to authenticate with work apps less frequently.
- When he browses to intranet websites, he is automatically authenticated and is not prompted for his username and password.
- He can access privileged apps that he is not able to log in to when he is out of the office.

When Bob leaves the office later that evening to go home, his device sends data to Persona that results in a new behavioral risk level and a new geozone risk level, with corresponding assignments to groups with profiles and permissions that are appropriate for that risk level.

Adapting device behavior in a defined geozone

Evan is in Vancouver on vacation. He has brought along his work device, an Android phone, so that he can keep up on his emails. Because he is currently located outside of the range of his typical learned geozones, the BlackBerry Persona services assess his geozone risk level to be high. As a result, the Persona policy that is applied to Evan's device takes effect and assigns Evan to a group with more restrictive device policies and profiles. His access to work apps and intranet sites is very limited and he has to sign in to work apps with both a password and BlackBerry 2FA authentication.

Evan decides to spend one day of his vacation visiting his company's Vancouver office so that he can meet a few coworkers and attend an important meeting. A Persona administrator has created a defined geozone for the Vancouver office and configured it with a static low risk level.

While Evan is visiting the office, the Persona policy executes the group assignment that Evan's administrator configured for this low-risk office location. Evan has unrestricted access to his work apps and intranet sites, and he can use single sign-on authentication for his work apps.

Confirming a user's identity

Michael is the main point of contact for an important project that his team is working on. He regularly fields questions and requests from key stakeholders within the company.

As Michael travels between offices to work with different team members and meet with project contacts, he uses BlackBerry Work to keep up with his emails. Two weeks ago, Michael's company implemented BlackBerry Persona. His administrator enabled the continuous authentication feature.

As Michael has been using BlackBerry Work, Persona has been collecting data about how he uses the app, including the physical gestures and the app features that he typically uses. Persona has used this information to train and develop a model that characterizes how Michael uses BlackBerry Work on a daily basis.

Michael is currently out of the office attending a conference. While he is having a discussion with a prospective customer, he sets his unlocked Android device on a table. Malcolm, an employee from a competing company, steals Michael's device.

Malcolm quickly leaves the conference hall and opens BlackBerry Work on Michael's device. He forwards several confidential emails to his own email account. Persona recognizes this as abnormal behavior that does not fit Michael's usage model; Michael rarely forwards emails to other people. Persona immediately triggers a reauthentication request in BlackBerry Work. BlackBerry Work and all other BlackBerry Dynamics apps on Michael's device are blocked until the correct password or fingerprint is provided.

Legal notice

©2020 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