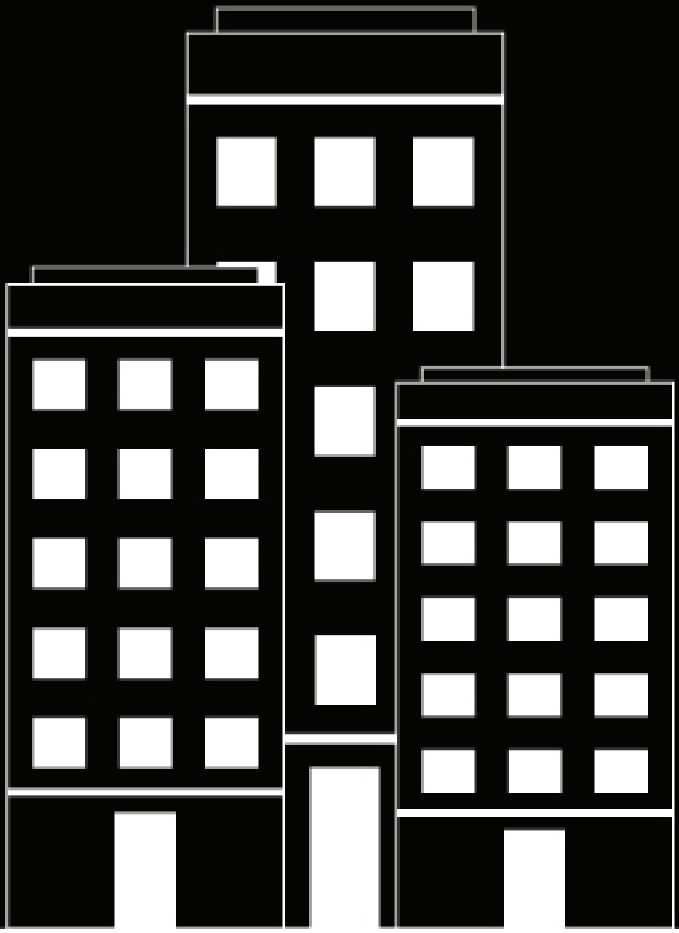

BlackBerry Persona Desktop

Administration Guide

Console 1.6 and Agent 1.2

Contents

What is BlackBerry Persona Desktop?

BlackBerry Persona Desktop is a local service that continuously authenticates a user's behavior while they are using a device. Persona Desktop creates a behavioral model of the user's activity and uses that model to recognize deviations from the user's expected behavior. If the activity deviates enough, Persona Desktop will require the user to reauthenticate themselves before they can continue to use the device. For example, if a malicious user gets access to a Persona Desktop device, their actions would not match the user's, and they would be locked out of the device.

Using Persona Desktop and BlackBerry Protect Desktop provides security against malicious users and malicious files.

Persona Desktop data models include:

- Keystroke data: the way the user types on the keyboard
- Mouse data: the way the user moves and clicks the mouse or trackpad
- Process start data: the applications the user launches and when
- Logon data: when the user logs on or when the user fails at logging on
- Network data: the IP addresses and ports the user accesses

A user's behavior contributes to a risk score based on their behavioral model. Administrators can set thresholds for how low a user's risk score can be before they must reauthenticate. Authentication could be a username and password or a two-factor authentication challenge. Administrators can also reset a user's score or temporarily pause Persona Desktop if someone needs to troubleshoot the device.

Does BlackBerry Persona Desktop collect or store personally identifiable information?

Persona Desktop does not record or store any personally identifiable information (PII). For example, the keyboard model analyzes behavioral usage of the keyboard, but it does not record which keys are pressed.

Configuring and using BlackBerry Persona Desktop

You complete the following steps to enable and use BlackBerry Persona Desktop in your organization's BlackBerry Cylance console.

1. Create a Persona Desktop custom role and assign it to the users who will manage the service.
   Administrators with global permissions can also manage the service.
2. Create a policy with CylancePERSONA enabled and do not add any mitigation actions. This is called a passive policy and is used while the model is training.
   You can add users to the Admin Safe List. For example, IT staff who may need to log on to the device to resolve issues.
3. Install BlackBerry Protect Desktop version 1574 or later on users' devices.
4. Install BlackBerry Persona Desktop on users' devices.
5. Assign the passive Persona Desktop policy to the devices.
6. In the console, check **Assets > Users** to see a list of Persona Desktop users who have logged in to their devices.
7. Allow the Persona Desktop models to run in training mode.

8. After the Persona Desktop models have completed training mode, assign the active Persona Desktop policy to the users' devices.
9. Create a policy with CylancePERSONA enabled, add mitigation actions, and add users to the Admin Safe List, if needed. This is called an active policy and is used after the model has been trained.

System Requirements

The following items are required to use BlackBerry Persona on a device.

Requirement	Description
BlackBerry Protect agent	Agent version 1574 or later For more information about hardware and software requirements to run the Protect Desktop agent, see the system requirements in the BlackBerry Protect Desktop Installation Guide.
Operating system	Microsoft Windows 10 Fall Creators Update (version 1709, Redstone 3, build 10.0.16299) or later **Note:** Persona Desktop supports only one user per device. Multiple user logins or using Terminal Services to share the device is not supported. One user can have multiple devices.
Software	• Microsoft .NET 4.6.2 or later • .NET Standard 2.0 or later • Microsoft Visual C++ 2017 Re-distributable or later (Persona Desktop will install Visual C++ 2017 re-distributable if needed)
Domain user account	The Persona Desktop login uses the domain user account
Physical machine	Physical machines are supported. **Note:** Virtual machines are not supported

Installing the Agent

A Cylance console administrator can download the Persona Desktop agent from the console. Administrators can install the agent manually on the device or through software management, like Microsoft System Center Configuration Manager (SCCM).

Because the Protect Desktop agent must be installed, the Persona Desktop agent does not require an installation token.

Download Persona

1. In the console, click **Settings**.
2. Click **Deployments**.
3. Select the following for the installer:
    - Product: CylancePERSONA
    - OS: Windows
    - Version: Select the version you want to install
    - Format: Select x64 or MSI
4. Click **Download**.

Install the Agent

Before you begin: BlackBerry Persona requires BlackBerry Protect for Desktop version 1574 or higher.

1. On the device, double-click the Persona Agent installer.
2. Follow the installation steps.

    If you want to allow a third-party app such as Cisco AnyConnect to run before you log in, type the GUID for the app in the **3rd Party App Whitelisting** screen. You can find the GUID in the Registry, in the Authentication folder.

- The installer does not have any messaging about completing successfully.
- To check that the Persona Desktop agent is installed:
    - The Cylance User Provisioning icon displays in the system tray.
    - The Persona Desktop user displays in the Users list on the Assets page in the Console.
    - Use Windows Task Manager and check that the CyPersona process is running.

After you finish:

- To uninstall the agent, use the Windows Settings.
- To update the agent, use the Zone-based Updating feature in the console.

Set up multifactor authentication

You can set up multifactor authentication for Persona Desktop using a FIDO key or Google Authenticator.

1. Navigate to the Persona Desktop Provisioning app (C:/Program Files/Cylance/Persona/).
2. Double-click the Provisioning app to open it.

3. Do one of the following:

To use a FIDO key:

a. Click the FIDO tab.
b. Insert your FIDO key into a USB port on your computer.
c. Type a nickname for the key.
d. Click **CONTINUE**.

To use Google Authenticator:

a. In the console, click the Google tab.
b. Type a nickname for the authenticator.
c. Click **CONTINUE**.
d. On your mobile device, download the Google Authenticator app from Google Play or the App Store.
e. Open the app and tap **Get started**.
f. Tap **Scan a QR code** and scan the QR code, or tap **Enter a setup key** and type R43V SHFF YT25.
g. Type the six-digit code generated by Google Authenticator.
h. In the console, click **AUTHENTICATE**.

Log in to Persona Desktop

Log in to the device using the Windows login screen. The Persona Desktop login uses the domain user account.

- If the user fails to login, they are not given access to the device.

Persona Desktop user trust score

With Persona Desktop installed, the agent creates behavioral model of the user's activity and uses that model to recognize deviations from the user's expected behavior. The model uses a score from 0 to 100, with 100 being a perfect match to the user's behavioral model.

Persona Desktop data models include:

- Keystroke model: the way the user types on the keyboard
- Mouse data: the way the user moves and clicks the mouse or trackpad
- Process start data: the applications the user launches and when
- Logon data: when the user logs on or when the user fails at logging on
- Network data: the IP addresses and ports the user accesses

Training mode

When Persona Desktop is first installed on a device, there is a period of time when the data models must be trained by the user's behavior. While in training mode, the Persona Desktop policy should be in a passive mode, which means mitigation actions are disabled in the policy. This will allow the model to train without triggering any authentication events.

Even during training mode, if the user fails to log in to the device, an alert will display in the console.

The Persona Desktop model training should take one to two weeks for most users. Training depends on the level of activity the user provides. The more activity, the sooner the model training completes.

Note: Users should not artificially inflate their activity to try to get the model to train faster; this could cause issues with the trust score. Users should go about their day as usual.

User trust score thresholds

In a policy, a console administrator can set a value for the user's trust score that will trigger a mitigation action if the user's trust score falls below that value. Up to two mitigation actions can be added to a policy.

- Prompt for username and password: requires the user to enter their username and password to access the device
- Prompt a second-factor challenge: requires the user to pass a two-factor authentication challenge to access the device; Persona Desktop currently supports Google Authenticator and FIDO

Tenant statistics chart

The tenant statistics chart appears on the Persona Desktop dashboard. It displays information about the number of events and the number of devices online over time. A device is counted as online if the cloud receives at least one event or score from the device in the specified period.

Note: If you use any of the filters at the top of the page, the alerts list on the left is refreshed and the details of the first alert on the list appear in place of the tenant statistics chart. To display the chart again, click on the Persona Desktop icon on the menu bar.

You can use the data shown on this chart to determine:

- Whether any large-scale events or trends are occurring in the BlackBerry Persona tenant
- Whether changes in events are correlated to user volume
- The number of events compared to the number of online users

You can click on the following items in the legend at the top of the chart to toggle them on and off in the graph:

- Failed 2FA Logon
- Forced Step-Up Authentication
- User Failed Logon
- # of Online Devices

You can select Last 30 Days to display the data as a total for every day or Last 24 Hours to display the data as a total for every hour. Hover the mouse pointer over a point to display its exact value.

Lowest trust score dashboard

The Persona Desktop displays a dashboard that shows the top ten users with the lowest trust score. The trust score displayed is the lowest trust score for a user on one of their devices. Each username is a link to the user details page.

Creating Persona Desktop policies

Policy settings control what the Persona Desktop agent will do on the device. You can create a new policy or edit an existing policy to change the Persona Desktop settings.

Add a mitigation action

When you first use Persona Desktop, it is recommended to test without adding mitigation actions; this is known as a passive policy. This will allow you to see what Persona Desktop will alert on without impacting your users with mitigation actions. After your testing is complete, add mitigation actions to the policy.

Note: After a user reauthenticates due to a mitigation action, Persona does not trigger another mitigation action for 60 minutes, unless the user crosses the next threshold. If a second mitigation action is triggered, Persona does not trigger another mitigation action for 60 minutes, regardless of the trust score during those 60 minutes.

1. In a policy, select the **CylancePERSONA Settings** tab.
2. Select the **CylancePERSONA** checkbox.
3. Click **Add Mitigation Action**.
4. Enter a value between 10 and 90.
   If the user's score falls below this value, the selected mitigation action is triggered.
5. Select a mitigation action. Up to two mitigation actions are allowed per policy.
   a) This can be a prompt for a username and password and a second-factor challenge, or two prompts for a username and password.
   b) When you add a second-factor challenge, select either Google Authenticator or FIDO.

      Note:

      - When you add a username and password prompt and a second-factor challenge, the username and password prompt value must be higher than the second-factor challenge value. A successful second-factor challenge resets the trust score, so having a username and password with a lower value would never be triggered.
      - Two second-factor challenges are not allowed because a successful second-factor challenge resets the trust score. Having a second, lower value second-factor challenge would never be triggered.
6. Click **Submit**.

After you finish:

- To edit an action, click the Edit icon.
- To delete an action, select the check box beside the action and click **Remove From List**.

Add Admin Safe List

Adding a username to the Admin Safe List allows that user to log on to a device and their actions will not count towards the trust score.

For example, you can add an administrator to this list so that they can to log on to a device to troubleshoot issues without affecting the trust score on the device.

1. In a policy, select the **CylancePERSONA Settings** tab.
2. Click the checkbox to enable the feature.
3. Click **Add Admin**.

4. Type in the username.
5. Click **Submit**.

After you finish:

- You can edit the username by clicking the edit icon.
- You can delete a username by selecting the checkbox, then clicking Remove From List.

Managing alerts

Note: Persona Desktop Alert data is retained for 90 days in the Console.

BlackBerry Persona Desktop alerts appear in the Console on the CylancePERSONA tab. The alerts are sorted by Action, Severity, and time. New alerts with the highest severity that are the most recent are listed first.

The Action sort order is:

- New (first)
- In Progress
- Reviewed
- False Positive (last)

You can view alerts for a Persona user on the Users page under Assets. The User Info page includes a list of alerts associated with the user. There is also a list of devices that are associated with the Persona user.

Item	Description
Severity	The Persona Desktop page lists the alerts by severity, with new Critical alerts displaying first. Alerts marked as Reviewed or False Positive displays after the New and In Progress alerts. Sort alerts by a date range or by username.
Action	Setting an Action for a Persona alert provides a workflow from new alerts to reviewed. • New • In Progress • Reviewed • False Positive
Date Range	• Click on the Date Range. The date range selector displays. • Select a From date and a To date. • Click Apply.
Username	• Click Username. • Type a username, then press Enter. The username is added under the search field. • Add additional usernames to filter the Alerts. Remove a username by clicking X.

Filter alerts

On the alerts page, you can filters the alerts to quickly find and work on the alerts you need to. You can filter alerts by alert type, date range, severity, status, and username.

Item	Description
Alert type	- Click Alert type. - Select one or more of the available alert types. The alert list updates as alert types are selected.
Clear all filters	Use to clear all alert filters.
Date range	- Click on the Date Range. The date range selector displays. - Select a From date and a To date. - Click Apply.
Severity	- Click Severity. - Select one or more of the available severity levels. The alert list updates as severity levels are selected.
Status	- Click Status. - Select one or more of the available status types. The alert list updates as status types are selected.
Username	- Click Username. - Type a username, then press Enter. The username is added under the search field. Enter at least three characters into the search field. - Add additional usernames to filter the Alerts. Remove a username by clicking X.
Zone	- Click Zone. - Type a zone name, then press Enter. The zone name is added under the search field. Enter at least three characters into the search field. - Add additional zones to filter the Alerts. Remove a zone by clicking X.

Alert details

On the Persona page, selecting an alert displays the alert details. This displays details about the user's trust score and the user's trust score log, a graph that shows the user's trust score over time.

Detail	Description
Alert Type	This is the alert Action Type and it is used as the name for the alert. See Alert Types for more information.
Severity	This is the severity of the alert.
Date / Time	This is the date and time the alert was recorded.
Username	This is the username associated with the alert.
Device Name	This is the device name associated with the alert.

Detail	Description
Current Trust Score	This is the user's current trust score on the device.
Lowest Trust Score	This is the lowest trust score for the user on the device in the last 24 hours.
IP Address	This is the IP address for the device.
Action	This is the action status of the alert.
User's Trust Score Log	This is the user's trust score and meta model.
Last 24 HRS / Last 30 Days	This is the user's trust score, represented by a graph for the last 24 hours or the last 30 days.
Related Alerts	This is for any alerts related to the current alert.
History & Comments	This lists the history of the alert and any comments related to the alert. New alerts and changes to an alert's status cause the system to generate a comment. Administrators can manually add comments, but can delete only their own comments.

Alert types

Alert types are the alert names that display in the console. See the table below for more details about each alert type.

Alert	Description	Severity
Forced Step-Up Authentication (Mitigation Triggered)	The user was required to enter their username and password or pass a 2FA challenge to continue using the device.	Low
User Failed Logon	The user failed to enter the correct username and password when logging into the device.	Low
Failed 2FA Logon	The user failed to pass the two-factor authentication (2FA) logon.	High

Related alerts

When viewing a Persona Desktop event, a Related Alerts tab displays under Additional Content. The related alerts are listed so administrators can see if there is a history of related events for this issue or if this is an isolated event.

Clicking a link in the Related Alerts list will display the associated information.

- **Alert** - Displays the alert details.
- **Device** - Displays the device details page (**Assets > Devices**).

- **Username** - Displays the user info page (**Assets > Users**).

Configure syslog settings

You can configure BlackBerry Persona Desktop to forward events to a syslog server. For information on configuring syslog and SIEM settings, see Syslog/SIEM settings in the BlackBerry Protect Desktop Administration Guide.

Each alert message sent to syslog contains:

- Event Type
- Event Name
- Tenant ID
- Alert ID
- Alert Type
- Alert Severity
- User ID
- User Name
- Device ID
- Device Name
- IP Address
- Alert Time
- User Trust Score
- Meta Model Score
- Keyboard Model Score
- Mouse Model Score
- Logon Model Score
- Process Model Score
- Network Model Score

Note: Trust scores and model scores are displayed as N/A in the syslog message when Persona Desktop is in training mode.

1. In the management console, click **Settings > Application** from the menu.
2. Select the Syslog/SIEM checkbox.
3. Select the **Persona Alerts** and type in any server information needed.
4. Click **Save**.

Managing Persona users

Persona users are listed on the Assets page in the console. Persona users are added when they log in to their devices for the first time.

- A Persona device can have one user associated with it. A Persona user can have multiple devices.
- Persona Desktop users are not console users. Persona Desktop users are listed under Assets because they do not have any access to the console.
- A Persona Desktop user is considered offline after 5 minutes of inactivity on the device.
- When a Persona Desktop user is removed from the console, all Persona Desktop data related to that user is also removed from the console.

View Persona users

1. In the console, select **Assets > Users**.

   The console displays the username, the state of the user (online or offline), the time when the user was last online, and the zones the user is a member of.
2. Select a username to view the User Info page. Do any of the following:
   - View User Info
   - View Persona Desktop alerts
   - View Associated Devices
     - Expand the device to see Persona Desktop info
   - Pause scoring for Persona Desktop on a device when an administrator logs on to the device to troubleshoot. This prevents the administrator's actions from influencing the Trust Score on that device. Remember to Resume the scoring when troubleshooting is complete.
   - Reset the Trust Score for a user on a device.

After you finish:

- Click a column heading to sort the Assets table.
- Click ≡ beside a column to filter the entries in that column. A green dot indicates that a filter is active. To remove a filter, click the x beside the filter above the list of users.
- To remove a Persona Desktop user, select the checkbox next to the username, then click Remove.

Note:

- If a Persona Desktop user is removed from the Assets list, but the Persona Desktop agent is not removed from the device, if the user logs in to the device, they will be added back as a Persona User asset when the agent communicates with the console.
- If the user never logs on using that device, or if the device is repurposed for a different user, this issue will not occur.

Zone Details page

You can manage Persona Desktop users on the Zone Details page. The page displays the following information:

Number of users - The number of Persona Desktop users assigned to a zone is displayed on the Zone Details page, along with the number of unsafe threats and number of devices.

Users tab - The Zone Details page has a tab for Persona Desktop users. This tab lists all Persona Desktop users assigned to the zone.

Filter the user list - You can filter the columns for the Persona Desktop user list on the Zone Details page. Filter by the username, state (online or offline), or by zone.

Add users to a zone

1. In the console, select a zone. The Zone Details page is displayed.
2. Click the **Users** tab.
3. Click **Add user to zone**.
4. Select one or more users to add to the zone. To select all users in the the list, select the checkbox beside the Username column.

   You can select a maximum of 100 users.
5. Click **Save**.

Remove users from a zone

1. In the console, select a zone. The Zone Details page is displayed.
2. Click the **Users** tab.
3. Select one or more users to remove from the zone. To select all users in the the list, select the checkbox beside the Username column.

   You can select a maximum of 100 users.
4. Click **Remove user from zone**. A confirmation dialog box is displayed.
5. Click **Remove**.

Using the BlackBerry Support Collection Tool

If you are working with BlackBerry Support to resolve an issue, you can download the BlackBerry Support Collection Tool to gather product data and system information. For more information, visit support.blackberry.com to read article 66596.

Legal notice

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