Cylance Endpoint Security

CylancePROTECT Desktop 3.x Upgrade Guide

Contents

Benefits of upgrading to CylancePROTECT Desktop 3.x

CylancePROTECT Desktop version 3.x represents a significant leap forward for the product, introducing new features and usability enhancements to keep your organization's data and devices secure.

Upgrading to CylancePROTECT Desktop for 3.x will give you access to the following features:

Windows

Feature	Description
OS compatibility	The Windows 3.x agent adds support for Windows 11. For more information, see the CylancePROTECT Desktop compatibility matrix.
Agent enhancements	• The Windows 3.1 agent runs as a trusted service using Antimalware Protected Process Light (AM-PPL) technology from Microsoft, which protects the agent's security processes from malicious actions. For example, it helps protect the agent from being terminated. This feature requires the endpoint to be running Windows 10 1709 or later, or Windows Server 2019 or later. • The Windows 3.2 agent reports a list of applications that are installed on endpoint devices to the management console. This feature allows administrators to identify applications that are installed on endpoint devices that may be a source of vulnerabilities, prioritize actions against vulnerabilities, and address them accordingly. Administrators can view all applications that are installed on endpoints that are registered with the tenant and view a list of applications that are installed on individual endpoints. This feature can be enabled from the device policy (agent settings).

Feature	Description
Memory protection enhancements	• New capabilities have been added to violation types, resulting in the generation of more events. • The “Injection via APC” violation type is available in the memory protection settings of a device policy. This option enables CylancePROTECT Desktop to detect a process that is injecting arbitrary code into the target process using an asynchronous procedure call (APC). For more information, see KB 92422. • The “Memory Permission Changes in Child Processes” violation type is available in the memory protection settings of a device policy. This option enables CylancePROTECT Desktop to detect when a violating process has created a child process and has modified memory access permissions in that child process. • Usability for memory protection controls has been improved. • Improved detection of LSASS read violations for Windows devices. • The size limit for memory protection exclusions has been increased from 64 KB to 2 MB, allowing you to add more exclusions. • Exclusions for third-party application DLLs are now supported to allow third-party apps to run alongside CylancePROTECT Desktop. For example, if you are running third-party security products in addition to CylancePROTECT, you can add an exclusion for the appropriate .dll files so that CylancePROTECT ignores specific violations for those products. This feature requires agent 3.1.1001 or later. For more information, see the Treat as DLL exclusion setting in the memory protection device policy. • The memory protection sensor for the malicious payload violation type has been improved to help improve accuracy of violation reporting and reduce unnecessary alerts. This feature requires agent 3.1.1001 or later.
Protection enhancements	• Windows 3.1 agent supports the ability for administrators to set a custom interval to run background threat detection scanning from the device policy (protection settings). The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. Note that increasing the frequency of the scans may impact the device performance. • Windows 3.2 agent supports the ability for administrators to initiate a background threat detection scan on demand from the management console. The command can be sent from the Device Details screen for an individual device, or for multiple devices at once from the Devices screen. • The date of the last scan for each device is logged in the management console.

Feature	Description
Script control enhancements	• You can select whether you want CylancePROTECT Desktop to alert on or block Python (2.7, 3.0 to 3.8) and .NET DLR scripts (for example, IronPython), and you can turn off script control for these script types. • Embedded VB scripts that caused script control events were blocked in agent version 2.1.1580; detection of embedded VB script control violations has been disabled in agent 3.0.1000 and later. • The Windows 3.1 agent works with Microsoft's anti-malware scan interface (AMSI) so that when a potentially dangerous XLM macro is executed, threat information is reported to the management console, and the agent responds to the interface according to the device policy rules for script control events. For example, the agent responds whether to allow or block the macro from running. This feature is enabled from the Script Control > XLM Macros setting in the device policy and requires the device to be running Windows 10. Make sure to disable VBA macros in the Excel **File > Trust Center > Excel Trust Center > Macro Settings** menu. • The Windows agent reports parent and interpreter processes to the Cylance console when a potentially malicious script is executed. Administrators can add exclusions for either a parent process or interpreter process of a script to allow the script to run on a device. This feature requires agent version 3.1.1001. • The Windows 3.2 agent supports enhanced script control using script scoring. Scripts that have an unsafe or abnormal threat score can be intelligently blocked from executing and alerted to the management console. Administrators can configure the script control settings in the device policy to block scripts that CylancePROTECT considers to be unsafe or abnormal. • The Windows 3.2 agent supports Alert mode for PowerShell Console scripts, so that detected events are reported to the management console while still allowing them to run. Administrators can control the setting from the Script Control tab in the device policy using the PowerShell Console drop-down menu.
Macro detection enhancements	• In device policies, the macro detection feature for Windows devices has been moved from the Script Control tab to the Memory Actions tab (Exploitation > Dangerous VBA Macro) for devices running Windows agent version 2.1.158x or later. The previous script control option for 2.1.1578 and earlier supports the Alert and Block actions; the new memory protection option supports the Ignore, Alert, Block, and Terminate actions. • You can now add exclusions for the Dangerous VBA Macro violation type in the memory protection settings of a device policy. • Files that cause Dangerous VBA Macro violations are displayed in the management console, allowing you to identify offending documents and determine if you need to add them to the exclusion list.

Feature	Description
Device control enhancements	You can now allow read-only access to the following USB device types: • Still image • USB CD/DVD RW • USB drive • VMware USB passthrough • Windows portable device
Global safe list enhancements	Adding a SHA256 hash to the global safe list for scripts now masks any block events related to that hash from appearing in the management console.
Logging changes	Important log entries have been moved from the Debug log level to the Info log level.

Linux

Feature	Description
OS compatibility	The Linux 3.2.x agent adds support for the following Linux distributions: • Amazon Linux 2023 • Amazon Linux 2, kernel 5.10 The Linux 3.1.x agent adds support for the following Linux distributions: • Red Hat Enterprise Linux 9 and 9.1 • Oracle 9 and 9.1 • Oracle UEK 9 and 9.1 • Oracle 8.7 • Oracle UEK 8.7 • SUSE Linux Enterprise Server (SLES) 15 SP4 • Ubuntu 22.04 LTS The Linux 3.0.x agent adds support for the following Linux distributions: • Red Hat Enterprise Linux /CentOS 8.4 • Red Hat Enterprise Linux 8.5 • Oracle 8.4 • SUSE (SLES) 12 SP5 • SUSE (SLES) 15 SP2 and SP3 For more information, see the CylancePROTECT Desktop compatibility matrix. To view the full list of supported Linux kernels and drivers, download the Supported Linux Kernels spreadsheet.

Feature	Description
Background threat detection on-demand scan	Administrators can now initiate a background threat detection scan on demand from the management console. The command can be sent from the Device Details screen for an individual device, or for multiple devices at once from the Devices screen. This feature requires CylancePROTECT Desktop agent version 3.2. The date of the last scan for each device is logged in the management console.
Custom interval for background threat detection scanning	• Administrators can set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. • This feature requires CylancePROTECT Desktop agent version 3.1. • The date of the last scan for each device is logged in the management console.
Auto-update Linux Driver	• The CylancePROTECT Desktop agent 3.1.1000 for Linux devices can now request an update to the latest supported agent driver when an updated kernel is detected on the system. For example, if the Linux kernel is updated and the current installed agent driver does not support it, the agent can now automatically update the driver as soon as a compatible driver is released. • This feature requires CylancePROTECT Desktop agent version 3.1.1000 and the agent driver version 3.1.1000 or later. • To enable this feature, select the Auto-update Linux Driver option in the zone-based update rule from the Settings > Update menu in the management console.
Memory protection enhancements	• New capabilities have been added to violation types, resulting in the generation of more events. • Usability for memory protection controls has been improved. • The size limit for memory protection exclusions has been increased from 64 KB to 2 MB, allowing you to add more exclusions.

macOS

Feature	Description
OS compatibility	• The CylancePROTECT Desktop 3.2.x agent adds support for macOS 14 (Sonoma). • The CylancePROTECT Desktop 3.1.x agent adds support for macOS 13 (Ventura). • The CylancePROTECT Desktop 3.0.x agent adds support for macOS 12 (Monterey).

Feature	Description
Background threat detection on-demand scan	Administrators can now initiate a background threat detection scan on demand from the management console. The command can be sent from the Device Details screen for an individual device, or for multiple devices at once from the Devices screen. This feature requires CylancePROTECT Desktop agent version 3.2. The date of the last scan for each device is logged in the management console.
Custom interval for background threat detection scanning	• Administrators can set a custom interval to run background threat detection scanning from the device policy. The scan interval can be set between 1 and 90 days. The default scan interval is 10 days. • The date of the last scan for each device is logged in the management console.
Memory protection enhancements	• New capabilities have been added to violation types, resulting in the generation of more events. • Usability for memory protection controls has been improved. • The size limit for memory protection exclusions has been increased from 64 KB to 2 MB, allowing you to add more exclusions.

For more information about additional features for the latest 3.x agents, as well as a comprehensive list of fixed issues, see the Cylance Endpoint Security Release Notes.

To benefit from these enhancements and the improvements coming in future versions of CylancePROTECT Desktop, BlackBerry strongly recommends upgrading all devices with the 2.x.158x agent or earlier to the latest version of agent 3.x. This guide covers considerations and additional instructions for a successful upgrade.

Upgrading to CylancePROTECT Desktop 3.x

This section provides step-by-step guidance and best practices to ensure a successful upgrade to CylancePROTECT Desktop version 3.x.

Step	Action
1	Review the guidance for preparing your test environment.
2	Review the agent upgrade paths to determine the specific path that you need to follow.
3	Configure and test memory protection.
4	Configure and test macro detection (Windows only).
5	If necessary, migrate script control macro exclusions to the new memory protection configuration.
6	After you complete your testing and validation in the test environment, apply the upgrade and updated device policies to your production environment.

Preparing your test environment

- BlackBerry recommends testing the upgrade to CylancePROTECT Desktop for Windows 3.x in a dedicated testing zone before you deploy the upgrade to your production environment. For more information about zones, see Setting up zones in the Cylance Endpoint Security setup content.
- Set up your test devices with the apps and configurations that accurately represent your production environment.
- Create dedicated device policies that you will use for your testing zones and devices. You can create new device policies or copy and modify existing policies.
- Configure zone-based update rules in the management console to restrict the 3.x upgrade to the dedicated zones and devices that you plan to use for testing. For instructions, see Managing updates for the CylancePROTECT Desktop and CylanceOPTICS agents in the Cylance Endpoint Security setup content.
- BlackBerry recommends downloading the Support Collection Tool from KB 66596. If you contact BlackBerry Support for assistance, Support may ask you to run the tool to collect additional data.
- See the agent upgrade paths to determine the specific path that you need to follow.
- After you complete the configuration and testing activities in this guide and validate the upgrade in your test zones, you can apply the agent upgrade and the updated device policies to your production environment.

Upgrade paths for the CylancePROTECT Desktop 3.x agent

The following upgrade paths have been tested and are officially supported:

Upgrade path to Windows agent version 3.x

Current agent version	Upgrade path
2.0.154x	→ 2.1.157x → 3.2.1000
2.1.156x	→ 2.1.157x → 3.2.1000
2.1.157x	→ 3.2.1000
2.1.158x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

Upgrade path to Linux agent version 3.x

Current agent version	Upgrade path
2.1.157x or earlier	→ 2.1.158x → 2.1.159x → 3.2.1000
2.1.158x	→ 2.1.159x → 3.2.1000
2.1.159x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

Upgrade path to macOS agent version 3.x

Current agent version	Upgrade path
2.0.154x	→ 2.1.156x → 2.1.158x → 3.2.1000
2.1.156x	→ 2.1.158x → 3.2.1000
2.1.158x	→ 3.2.1000
2.1.159x	→ 3.2.1000
3.0	→ 3.2.1000
3.1	→ 3.2.1000

Configure and test memory protection

CylancePROTECT Desktop 3.x introduces various memory protection enhancements and increased visibility into the activity of the applications and processes on a device. In some situations, applications perform operations that could be considered malicious, but are performed for legitimate purposes. BlackBerry recommends following the steps and best practices below to ensure the proper tuning of the CylancePROTECT Desktop 3.x agent before you deploy it to your production environment. For more information about memory protection violation types, see Memory Protection in the Cylance Endpoint Security setup content.

1. In the management console, on the menu bar, click **Policies > Device Policy**.
2. Click the device policy for your test devices.
3. On the **Memory Actions** tab, select the **Memory Protection** check box.
4. In the **Violation Type** table, expand **Exploitation**, **Process Injection**, and **Escalation**. For all violation types listed under **Available for Agent Version 2.1.1580 and higher** and **Available for CylancePROTECT 3.0 and higher**, select the **ALERT** action.
5. Save the device policy.
6. Run CylancePROTECT Desktop 3.x on your test devices and review alerts to determine the risk of these exploits within your environment. If any of these alerts are low risk and will cause business impact, you can add targeted memory protection exclusions. For instructions and guidance, see Memory Protection.

   It is recommended that you restart each test device after you install or upgrade to CylancePROTECT Desktop 3.x.

After you finish: After you review alerts and add the necessary exclusions, you can change the violation type actions in the device policy as necessary (for example, Block or Terminate).

Configure and test macro detection (Windows only)

There are two options available in a device policy to detect and respond to potentially dangerous macros on Windows devices. The Macros option on the Script Control tab applies to Windows agent 2.1.1578 and earlier. The new Exploitation > Dangerous VBA Macro option on the Memory Actions tab applies to Windows agent 2.1.1580 and later. When you test your upgrade to agent 3.x, you must check your current configuration for detecting and responding to macros and configure the new Dangerous VBA Macro option accordingly.

1. In the management console, on the menu bar, click **Policies > Device Policy**.
2. Click your production device policy.
3. On the **Script Control** tab, note the current configuration for macros (Alert or Block).
4. In **Policies > Device Policy**, click the device policy for your test devices.
5. On the **Memory Actions** tab, expand **Exploitation**.
6. For the **Dangerous VBA Macro** violation type, set the appropriate action (Ignore, Alert, Block, or Terminate).
7. Save the device policy.
8. If necessary, migrate script control macro exclusions to the new memory protection configuration.
9. Run CylancePROTECT Desktop 3.x on test devices that use files with macros that are commonly used in your organization. If necessary, add additional memory protection exclusions for safe macros. For instructions and guidance, see Memory Protection in the Cylance Endpoint Security setup content.

Migrate script control macro exclusions to the new memory protection configuration (Windows only)

If you previously added macro exclusions on the Script Control tab of your device policies, you must migrate those exclusions to the new memory protection configuration for CylancePROTECT Desktop for Windows 3.x. If you

want to migrate the script control exclusions manually, you can simply record the exclusions you added on the Script Control tab of your device policies, then add the same exclusions on the Memory Actions tab in your device policies.

Follow the steps below if you want to migrate the existing script control exclusions using a PowerShell script that BlackBerry provides.

Note: The steps below apply to tenants managed using the Cylance console. If you manage tenants using the Multi-Tenant Console, see KB 92149.

Before you begin:

- Verify that PowerShell is installed on your computer and that PowerShell scripts are not blocked by security software, including CylancePROTECT Desktop. If CylancePROTECT Desktop is installed on your computer, in the device policy assigned to your device, verify that **Script Control > Block PowerShell console usage** is turned off.
- In the Cylance console, add an integration with the following API privileges and record the resulting application ID and secret:
  - **Policies**: Read, Modify
  - **Users**: Read
- In **Settings > Integrations**, record the **Tenant ID**.
- When you run the script, you will specify the email address of a Cylance console administrator account. Verify that the account that you want to use has the Administrator role.
- In the device policies where you want to migrate exclusions from script control to memory protection, verify that script control is enabled and that macro exclusions are present.
  - The script will ignore policies with script control disabled and policies that do not have any script control exclusions.
  - The script does not migrate exclusion lists with multibyte characters. You must add these exclusions manually.
- Download the PowerShell script.

1. Open a PowerShell command prompt and change the directory to the location of the script.
2. Run the script using the appropriate parameters from the table below.
   - Run the script in `-dryRun` mode first to preview the migration without making any changes. This will produce an output file that you can use to identify and correct any issues.
   - Run the script for the specific device policies that you plan to use for testing. After your testing and validation of the 3.x agent, you can use the script to apply the migration to your production device policies.

Parameter	Required or optional	Description
`-copySCExclusions`	Required	This command executes the migration of macro exclusions from the script control configuration to the new memory protection configuration.

`-allPolicies`
OR
`-policy '<policy_name>'`
	Required	`-allPolicies` executes the migration for all device policies in your tenant.
		`-policy '<policy_name>''` executes the migration for a specified device policy.

Parameter	Required or optional	Description
`-dryRun`	Optional	This command previews the execution of the script without making any changes. When you run the script in this mode, it creates an output file in the directory that the script is executed from.
`-tenantId '<tenant_ID>'`	Required	This command specifies the ID of your Cylance Endpoint Security tenant.
`-apiKey '<application_ID>'`	Required	This command specifies the application ID of the integration that you added in Settings > Integrations.
`-apiSecret '<application_secret>`	Required	This command specifies the application secret of the integration that you added in Settings > Integrations.
`-userEmail '<admin_email>'`	Required	This command specifies the email address of the Cylance console administrator account that you want to use to execute the migration. The account must have the Administrator role.
`-region '<region_code>'`	Required	This command specifies the region of your Cylance Endpoint Security tenant. Use one of the following values: • North America: `na` (default value if not specified) • Japan: `apne1` • Australia: `au` • Europe: `euc1` • South America: `sae1` • GovCloud: `us`
`-Ignore158xWarning`	Optional	This command makes the migration process ignore errors related to the size limit for memory protection exclusions, which has been increased from 64 KB for older versions of CylancePROTECT Desktop to 2 MB for version 3.x. **Note:** Use this parameter only if all devices that are associated with the target device policy use agent 3.x or later.

Parameter	Required or optional	Description
`-ignore158xCompatibility`	Optional	This command is related to a specific defect with CylancePROTECT Desktop for Windows 2.1.1580 and 1584 (see KB 88218). The fix for the defect (adding an additional asterisk(*) to the wildcard value in an exclusion path to make the wildcard **) is built into the script by default. If you use this parameter, the fix that is built into the script is disabled. **Note:** Use this parameter if the target device policy is associated with devices with agent 1578 or earlier and devices with agent 3.x or later. If the policy is associated with any devices with agent 158x, do not use this parameter.
`-includeExtensions <extensions>`	Optional	This command specifies the extensions to migrate to the memory protection configuration (for example, `-includeExtensions ps1, ja, xlxs`). If you don't use this parameter, all extensions are migrated.

Note: When you run the script in `-dryRun` mode, you may encounter the following error in the output file: "Entering Modify '<*policy_name*>' Policy... logError : The requested policy has not been converted to MemoryProtection v2." This can occur if a device policy has not been edited for some time. To resolve this issue, in the management console, open and save the policy.

The PowerShell output will indicate if any script control exclusions could not be migrated. You must add these exclusions to the memory protection configuration manually.

Example: Run the script in -dryRun mode

```
.\sc2memdef_copy.ps1 -copySCExclusions -allPolicies -
dryRun -tenantId '00000000-0000-0000-0000-000000000000' -
apiKey '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

Example: Run the script for a specific device policy

```
.\sc2memdef_copy.ps1 -copySCExclusions -policy 'userPolicy'
 -tenantId '00000000-0000-0000-0000-000000000000' -
apiKey '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

Example: Run the script for all device policies

```
.\sc2memdef_copy.ps1 -copySCExclusions -allPolicies -
tenantId '00000000-0000-0000-0000-000000000000' -apiKey
 '00000000-0000-0000-0000-000000000000' -apiSecret
 '00000000-0000-0000-0000-000000000000' -userEmail 'user@blackberry.com' -region
 'na'
```

After you finish:

- On the Memory Actions tab of the target device policies, check the migrated exclusions and delete any that do not apply to the new Dangerous VBA Macro violation type.
- Delete the PowerShell integration that you added to the management console.

Troubleshooting CylancePROTECT Desktop 3.x

Windows

Issue	Solution
The following error displays when you try to save a device policy after adding memory protection exclusions: “Could not save policy. Please try again”.	If the exclusion path includes a wildcard value that uses a single asterisk (*), modify the wildcard to add an additional asterisk (**), then try to save the policy again. For more information, see KB 94518.
The CylancePROTECT Desktop 3.0.1000 agent creates a large number of temporary files in the Windows temporary file directories.	Upgrade to agent 3.0.1005 or later. For more information, see KB 94849.
An unexpected number of processes are blocked after upgrading to CylancePROTECT Desktop 3.x.	For guidance and best practices, see KB 85991.

Linux

Issue	Solution

“Operation not permitted” errors when you try to install CylancePROTECT drivers	One of the following errors (or a similar error) displays in the Linux terminal when you install the CylancePROTECT drivers:
	`modprobe: ERROR: could not insert 'CyProtectDrvOpen': Operation not permitted`
	`modprobe: ERROR: could not insert 'CyProtectDrv': Operation not permitted`
	`Key was rejected by service`
	This error typically occurs when you try to install Linux drivers on a device that has Secure Boot enabled. For more information, see KB 73487.

Virtualization issues	The CylancePROTECT Desktop agent for Linux uses the BIOS serial number and the unique ID generated by dbus (machine-id) to generate a device fingerprint. Issues may occur in some VM environments that use a gold image. Linux machines that are generated from the gold image may retain identical BIOS serial numbers and IDs generated by dbus. This can cause VMs to check into the same device on the console instead of registering as a unique device. When encountering this issue, it is recommended to check the BIOS serial numbers and machine-ids of the cloned machine to ensure that these values are unique for each machine. For more information, see KB 66123.

macOS

Issue	Solution

System Extension is blocked when the CylancePROTECT Desktop agent runs	After upgrading a CylancePROTECT Desktop device with macOS 11.15.0 to a later macOS version, the following error occurs: “System Extension Blocked. A Program tried to load new system(s) signed by "Cylance, Inc." That needs to be updated by the developer.”
	
	This issue occurs because System Extensions must be enabled for the CylancePROTECT Desktop agent. Users must navigate to System Preferences > Security & Privacy, then click Allow for the Cylance extension.
	
	Organizations that are using JAMF to deploy CylancePROTECT Desktop may need to allow users to approve system extensions from within the JAMF configuration, using the following settings:
	
	• Enable “Allow users to approve system extensions”
	• Under “Allowed Team IDs and System Extensions”:
	  • Display Name: Cylance Protect
	  • System Extension Types: Allowed System Extensions
	  • Team Identifier: 6ENJ69K633
	  • Allowed system extensions: com.cylance.CylanceEndpointSecurity.extension

Legal notice

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