Quick Reference Guide

Integrating BES12 and Good Dynamics

Version 12.4

Published: 2016-02-12
SWD-20160212113853324

Contents

Integrating BES12 and Good Dynamics

1

This document outlines how to integrate BES12 and Good Dynamics. When you integrate BES12 and Good Dynamics, you can take advantage of Good's mobile app containerization and BlackBerry's cross-platform MDM capabilities.

When you integrate BES12 and Good Dynamics, you get unparalleled features and flexibility. For existing BES12 environments, here are some of the advantages you get when you integrate with Good Dynamics:

- Best-in-class secure mobile app platform and container
- Good Work and collaboration apps optimized for business-class user experience
- Ecosystem of more than 2000 secure mobile apps and Open API SDK
- Cross-platform support for iOS, Android, OS X, and Windows devices, desktops, and wearables

For existing Good Dynamics environments, here are some of the advantages you get when you integrate with BES12:

- Simplified Good Dynamics end-user enrollment experience
- Best-in-class MDM/MAM/EMM, including Apple DEP and VPP, BlackBerry Secure Gateway Service, and support for Samsung KNOX Workspace and Android for Work
- Comprehensive EMM platform, extensible to a rich portfolio of secure mobile apps and services, such as WatchDox, Strong Authentication, and Enterprise Identity by BlackBerry

Determining your integration path

Current environment	Path
You currently have a Good for Enterprise environment and want to take advantage of BES12 cross-platform MDM capabilities and simplified Good Dynamics end-user enrollment experience.	1. Upgrade to Good Control. For instructions on how to transition from Good for Enterprise to Good Control, see https://media.good.com/documents/gfe_transition_guide.pdf. 2. Steps to integrate your BES12 and Good Dynamics environments.
You currently have a Good Dynamics environment and want to take advantage of BES12 cross-platform MDM capabilities and simplified Good	Steps to integrate your BES12 and Good Dynamics environments

Current environment	Path
Dynamics end-user enrollment experience.	
You have a BES12 environment and want to take advantage of Good's best-in-class secure mobile app platform and container, including Good Work and collaboration apps optimized for business-class user experience.	Steps to integrate your BES12 and Good Dynamics environments

Steps to integrate your BES12 and Good Dynamics environments

When you integrate your BES12 and Good Dynamics environments, you perform the following actions:

Step	Action
1	Verify that your environment meets the device and server requirements.
2	In Good Control, deactivate device management on devices and disable MDM.
3	In Good Control, entitle Good for BES12, BES12 Client, and Good apps.
4	In Good Control, configure Exchange ActiveSync for Good Work.
5	In Good Control, select apps to authenticate for other apps.
6	In BES12, configure a connection to a Good Control server.
7	In BES12, create a Good Dynamics profile .
8	In BES12, add the Good apps for iOS devices or for Android devices.
9	In BES12, create an app group that contains all of the Good apps.

Step	Action
10	In BES12, create an activation profile.
11	In BES12, create any necessary user accounts.
12	In BES12, assign an app group to a user account.
13	In BES12, assign the activation profile to a user account.
14	In BES12, assign the Good Dynamics profile to a user account.
15	Instruct users to activate an Android device or activate an iOS device.

Verifying that your environment meets the device and server requirements

Before you can integrate BES12 and Good Dynamics, you must make sure that the following requirements are met:

- Good server requirements
- BES12 server requirements
- Device requirements

For additional requirements, see the Compatibility matrix.

Good server requirements

To access Good resources, you must create a Good Account at https://account.good.com/pce/#/register. If you are already registered with https://community.good.com, you do not need to create a new account.

Good server requirement	Where to find more information
Good Control server version 2.2.511.9 or later	For information about installing a Good Control server, refer to GD Server Installation at https://community.good.com/docs/DOC-1043.
Good Proxy server version 2.2.511.3 or later	For information about installing a Good Proxy server, refer to GD Server Installation at https://community.good.com/docs/DOC-1043.

Good server requirement	Where to find more information
Good licenses	Contact your BlackBerry account representative to get the latest details on packaging, pricing, and licensing.
To use additional services (for example, Good Connect, Good Presence, Good Push Notifications, Good Docs, Good Follow-Me, Good Directory Lookup, and Good Analytics), install the latest version of the Good Enterprise Mobility Server	For more information about installing a Good Enterprise Mobility Server, see the *GEMS Deployment Planning Guide* at https://media.good.com/documents/gems_deployment.pdf.

BES12 server requirements

BES12 server requirement	Where to find more information
BES12 version 12.4 or later	For information on installing BES12, see http://help.blackberry.com/en/bes12/12.4/installation-and-upgrade/steps_to_plan_your_BES12_environment.html.

Device requirements

Device requirement	Where to find more information
Android devices with the latest version of the BES12 Client installed.	For more information about the BES12 Client, refer to http://help.blackberry.com/en/bes12/12.4/security/dsc1411076924494.html.
iOS devices with the latest version of the Good for BES12 app installed.	
Any of the following licenses: • Silver SIM license • Gold SIM license • Silver server license • Gold - Secure Work Space server license	For more information about licensing, see http://help.blackberry.com/en/bes12/12.4/licensing/steps-to-use-licenses.html.

Device requirement	Where to find more information
• Gold server license • Gold - Flex server license **Note:** After the device is Good enabled, this license is released and no longer required. You do not have to purchase additional BES12 licenses.	

Good Secure EMM Suites

Good Secure EMM Suite licenses allow devices to use both BES12 and Good Dynamics features. The license names are different in *my*Account and BES12. In the Account Support > Advanced License Management section in *my*Account, the names reflect the Good Secure EMM Suite license names. On the Licensing summary page in the BES12 management console, the names reflect the corresponding BES12 license names listed in the following table. When you activate Good Secure EMM Suite licenses in BES12, the licenses are added to the total for the appropriate BES12 license. For example, if you have 50 Silver licenses and you activate 100 Good Secure Enterprise Suite licenses, the Licensing summary page displays a total of 150 Silver licenses. In later versions of BES12, the Licensing summary page will display the Good Secure EMM Suite license names.

Note: Good Secure EMM Suites provide user-based licenses, which allow a user to activate multiple devices with a single license. If you activate Good Secure EMM Suite licenses in BES12 version 12.4 or earlier, they are considered device-based licenses and a user requires a license for each device that they want to activate. For more information, contact BlackBerry support.

Good Secure EMM Suite subscription	BES12 license
Good Secure Management Suite	Silver
Good Secure Enterprise Suite	Silver
Good Secure Collaboration Suite	Gold - Flex
Good Secure Mobility Suite	Gold - Flex
Good Secure Content Suite	Gold - Flex

Connecting BES12 to a Good Control server

You can configure a connection between BES12 and a Good Control server instance to allow iOS and Android devices to access Good Dynamics productivity apps, such as Good Work, Good Access, and Good Connect.

In Good Control, deactivate device management on devices

To manage a user's devices in BES12, the user must not have any activated devices in Good Control. To deactivate devices in Good Control, you must remove the policy sets that are assigned to users. You must know the names of the device policies and any associated policy sets.

1. In Good Control, click **Policy Sets**.
2. Click the **Edit** icon beside the device policy that you want to remove.
3. Click **Device Management**.
4. In the **Device Policies** section, under **Actions**, click the **Delete** icon to remove the device policy from the policy set.
5. Click **Update**.
6. Click **Update**.
7. Repeat these steps for all affected policy sets and device policies.

In Good Control, disable MDM

Before you begin: In Good Control, deactivate device management on devices.

1. In Good Control, under **Settings**, click **Servers** > **Server Properties**.
2. Deselect **gc.mdm.enabled**.
3. Click **Submit**.
4. Restart the GC services. For instructions, see *Start or Restart the GC or GP Service* in the GC help.

In BES12, export the self-signed root certificate for the Good Control server

Complete the following task if the Good Control certificate has not been replaced with a third-party certificate. BES12 inherently trusts certificates from third-party providers, so you do not need to export the certificate from the Good Control server and import it in to BES12.

Note: The following task is not browser-specific. For specific instructions, see the documentation for the browser you are using.

1. In a browser, navigate to the login screen of any of your Good Control servers. A certificate error message is displayed because the CA that signed the certificate was Good Control, and the browser does not recognize it as a well-known CA.
2. Click or check the appropriate response to accept the security risk and open the Good Control console.
3. Log in to the Good Control server.
4. Open the Certificate dialog by clicking the certificate icon in the URL field.
5. Click **View certificate** or **Certificate information** to open the Certificate management menu.
6. Click the **Details** tab.
7. Select the root certificate. The root certificate is the first item in the Certificate hierarchy.
8. Click **Copy to file** or **Export**.
9. Make sure that the **DER encoded binary X.509 (.CER)** format is selected.
10. Enter a location and file name for the certificate. The common name of the Good Control root certificate must be the same as the FQDN of the Good Control host.
11. Click **Next** or **Save**.
12. Click **Finish**.

In BES12, configure a connection to a Good Control server

Before you begin:

- Verify that you have access to an administrator account on the Good Control server.
- In a browser, navigate to the Good Control console and export the Good Control server root CA certificate to your desktop. For instructions, see your browser's help documentation.

Note: If the Good Control server certificate has been replaced with a third-party certificate, you do not need to export the certificate from the Good Control server and import it to BES12. By default, BES12 trusts certificates from third-party providers.

1. In the BES12 management console, on the menu bar, click **Settings** > **Infrastructure** > **Good Control**.
2. In the **Server name** field, enter the name of the Good Control server.
3. In the **Username** field, enter the domain\username of the administrator account.
4. In the **Password** field, enter the password of the administrator account.
5. If necessary, click **Browse**. Navigate to and select the Good Control server root CA certificate.
6. Click **Save**.

Setting up Good Dynamics for devices

You can use the Good Dynamics profile to allow iOS and Android devices to access Good Dynamics productivity apps such as Good Work, Good Access, and Good Connect. You can assign the Good Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps.

The Good Dynamics profile is added to the BES12 management console when communication between BES12 and the Good Control server is configured. The profile allows you to enable Good Dynamics for users that are not already Good enabled.

In Good Control, entitle Good for BES12, BES12 Client, and Good apps

Users must be entitled to view or run the Good apps before they can be managed in BES12. Good Control has an Everyone group that automatically includes all users. The easiest way to entitle apps for all your users is to entitle the apps in the Everyone group.

Before you begin:

Your organization must have licenses and entitlements for Good Work, Good Access, Good for BES12 to activate iOS devices, BES12 Client to activate Android devices, and any other Good apps that you want users to install on devices.

1. In Good Control, under **Apps**, click **App Groups**.
2. Click the **Edit** icon beside **Everyone**.
3. Beside **Entitled Enterprise Apps**, click **Add More**.
4. In the **View** drop down box, select **All Applications**.
5. Select Good for BES12 for activating iOS devices, BES12 Client for activating Android devices, Good Work, Good Access, and any other Good apps that you are entitled to.
6. Click **OK**.

In Good Control, configure Exchange ActiveSync for Good Work

The Good Work app must be configured for Exchange ActiveSync. This allows your users to easily enroll in Exchange ActiveSync when they activate their Good Work app. For more information on how to configure Exchange ActiveSync for Good Work, see the *Good Work Product Guide for Administrators* at https://media.good.com/documents/goodwork_product_guide.pdf.

In Good Control, select apps to authenticate for other apps

You can select apps to act as the authenticator on behalf of other apps so that users do not have to create a password for each app that they install. For more information about delegating authentication, see https://media.good.com/documents/goodwork_product_guide.pdf.

1. In Good Control, under **Policies**, click **Policy Sets**.
2. Create a copy of the **Good Default Policy**.
3. Enter a name and description for the policy.
4. On the **Security Policies** tab, scroll to the **Authentication Delegation** section.
5. Click **Add Application**. From the list, select the app that your users use the most to act as the authentication delegate. Repeat this process to add up to three apps.
6. Select the **Allow self-authentication when no authentication delegate application is detected** option.
7. Click **Update**.

In BES12, create a Good Dynamics profile

Before you begin:

- In Good Control, entitle Good for BES12, BES12 Client, and Good apps
- In Good Control, select apps to authenticate for other apps

Complete the following task to create a Good Dynamics profile.

1. In the BES12 management console, on the menu bar, click **Policies and Profiles**.
2. Click + beside **Good Dynamics**.
3. Type a name and description for the profile.
4. In the **Good Control policy set** drop down list, select the policy set that you created in Good Control for authentication delegation.
5. If you entitled apps for the Everyone group in Good Control, you do not need to select an app group because the Everyone group is used by default. If you entitled apps to a custom app group in Good Control, click + under **Good app group**. to select the group.
6. Click **Add**.

Creating the Good Dynamics profile does not automatically update user accounts and devices. The Good app group and Good Control policy set selected in the profile take effect when the user is created in Good Control through BES12.

In BES12, add the Good apps for iOS devices

Before you can assign the Good apps to users, you must add the apps to BES12.

1. In the BES12 management console, on the menu bar, click **Apps**.
2. Click .
3. Click **App Store**.
4. In the search field, search for Good Work.
5. In the drop-down list, select the country of the store that you want to search in.
6. Click **Search**.
7. In the search results, click **Add** beside the Good Work app.
8. In the **Supported device form factor** drop-down list, select the form factors that the app can be installed on. For example, you can prevent the app from being available in the Work Apps app for iPad.
9. If you want the app to be deleted from the device when the device is removed from BES12, select **Remove the app from the device when the device is removed from BES12**. This option applies only to apps with a disposition marked as required and the default installation for required apps is set to prompt once.
10. If you want to prevent apps on iOS devices from being backed up to the iCloud online service, select **Disable iCloud backup for the app**. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.
11. In the **Default installation for required apps** drop-down list, perform one of the following actions:
    - If you want users to receive one prompt to install the app on their iOS devices, select **Prompt once**. If users dismiss the prompt, they can install the app later.
    - If you don't want users to receive a prompt, select **No prompt**.

    The default installation method applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.
12. In the **Convert installed personal app to work app** drop-down list, select one of the following:
    - To convert the app to a work app if it is already installed on iOS 9 or later devices, select **Convert** to convert the app. After you assign the app to a user, the app is converted to a work app and can be managed by BES12.
    - If you don't want to convert the app to a work app if it is already installed on iOS 9 or later devices, select **Do not convert**. After you assign the app to a user, the app cannot be managed by BES12.
13. Click **Add**.
14. Repeat these steps for Good Access and any other Good apps that you want users to install on devices.

In BES12, add the Good apps for Android devices

1. In the BES12 management console, on the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. Click **Open Google Play** and search for **Good Work**.
5. Click the Good Work app, copy the URL, and save the icon to a location on your computer.
6. In the **App name** field, type **Good Work**.
7. In the **App description** field, type a description for the app.
8. In the **Vendor** field, type the name of the app vendor.
9. In the **App icon** field, click **Browse**. Locate the Good Work icon that you saved to your computer.
10. In the **App web address from Google Play** field, paste the web address of the Good Work app.
11. To add screen shots of the app, click **Add** and browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
12. In the **Send to** drop-down list, select **All Android devices**.
13. Click **Add**.
14. Repeat these steps for Good Access and any other Good apps that you want users to install on devices.

In BES12, create an app group that contains all of the Good apps

Before you begin:

- In BES12, add the Good apps for iOS devices
- In BES12, add the Good apps for Android devices

1. In the BES12 management console, on the menu bar, click **Apps**.
2. Click .
3. Type a name and description for the app group.
4. Click .
5. Select the Good apps that you added to BES12.
6. Click **Add**.
7. Click **Add**.

In BES12, create an activation profile

You can control how devices are activated and managed using activation profiles. An activation profile specifies how many and what types of devices a user can activate and the type of activation to use for each device type.

1. In the BES12 management console, on the menu bar, click **Policies and Profiles**.
2. Click + beside **Activation**.
3. Type a name and description for the profile.
4. In the **Number of devices that a user can activate** field, specify the maximum number of devices the user can activate.
5. In the **Device ownership** drop-down list, perform one of the following actions:
    - If some users activate personal devices and some users activate work devices, select **Not specified**.
    - If users typically activate work devices, select **Work**.
    - If users typically activate personal devices, select **Personal**.
6. Optionally, select an organization notice in the **Assign organization notice** drop-down list. If you assign an organization notice, users activating iOS devices must accept the notice to complete the activation process.
7. In the **Device types that users can activate** section, deselect **BlackBerry** and **Windows**.
8. In the **Activation type** section, select the activation profile that you want to user for iOS and Android devices:

Activation type	Description
MDM controls	A separate work space is not created on devices. Administrators have basic management controls using options that are native to iOS and BES12 provides the MDM profile to the Good for BES12 app.
User privacy	MDM control of the device is not required (for example, BYOD devices) and users' personal data remains private. Devices activated with User privacy are activated on BES12 and can use services such as Find my Phone and Root Detection, but administrators cannot control device policies.

To activate a device on BES12, one of the following licenses is consumed:

- Silver SIM license
- Gold SIM license
- Silver server license
- Gold - Secure Work Space server license
- Gold server license
- Gold - Flex server license

After the device is Good enabled, this license is released and no longer required.

9. Click **Add**.

In BES12, create a user account

Users that do not exist in Good Control are automatically created when they activate devices using the Good for BES12 app on iOS devices or BES12 Client on Android devices. If a user is deleted from BES12 after they have activated a device, the user is also deleted from Good Control.

Before you begin:

- If you want to add a directory user, verify that BES12 is connected to your company directory. The same company directory must also be configured for Good Control.
- If you did not configure the company directory when you installed Good Control, you must add it to Good Control. For more information about the "authenticator.adsi.domains.additional" property, see the *GC Server Property Reference* the in the Good Control online help.

1. In the BES12 management console, on the menu bar, click **Users**.
2. In the left pane, click **Add user**.
3. Perform one of the following tasks:

Task	Steps
Add a directory user	1. On the **Company directory** tab, in the search field, specify the search criteria for the directory user that you want to add. You can search by first name, last name, display name, username, or email address. 2. Click 🔍. 3. In the search results, select the user account.
Add a local user	1. Click the **Local** tab. 2. In the **First name** field, enter a first name for the user account. 3. In the **Last name** field, enter a last name for the user account. 4. In the **Display name** field, make changes if necessary. The display name is automatically configured with the first and last name that you specified. 5. In the **Username** field, enter a unique username for the user account. 6. In the **Email address** field, enter a contact email for the user account.

4. If local groups exist in BES12, and you want to add the user account to groups, in the **Available groups** list, select one or more groups and click →.

When you create a user account, you can only add it to local groups in BES12. If the user account is a member of a directory-linked group, it is automatically associated with that group when the synchronization between BES12 and your company directory occurs.

To add a user account to groups that are assigned an administrative role, you must be a Security Administrator.

5. If you add a local user, in the **Console password** field, enter a password for BES12 Self-Service. If the user is assigned an administrative role, they can also use the password to access the management console.
6. Perform one of the following tasks:

Task	Steps
Automatically generate an activation password for the user and send an activation email	1. Select the **Autogenerate device activation password and send email with activation instructions** option. 2. In the **Activation period expiration** field, specify the number of minutes, hours, or days that the user can activate a device before the activation password expires. 3. In the **Activation email template** drop-down list, click a template to use for the activation email.
Set an activation password for the user and, optionally, send an activation email	1. Select the **Set device activation password** option. 2. Enter an activation password. 3. In the **Activation period expiration** field, specify the number of minutes, hours, or days that the user can activate a device before the activation password expires. 4. Perform one of the following actions: a To send activation instructions to the user, in the **Activation email template** drop-down list, click a template to use for the activation email. b If you do not want to send activation instructions to the user, clear the **Send email with activation instructions and activation password** check box. You must communicate the activation password to the user.
Do not set an activation password for the user	1. Select the **Do not set device activation password** option. You can set an activation password and send an activation email later.

7. If you use custom variables, expand **Custom variables** and specify the appropriate values for the variables that you defined.
8. Perform one of the following actions:
    - To save the user account, click **Save**.

- To save the user account and create another user account, click **Save and new**.

In BES12, assign the Good Dynamics profile to a user account

Before you begin:

- In BES12, create a Good Dynamics profile

1. In the BES12 management console, on the menu bar, click **Users**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the **IT policy and profiles** section, click +.
5. Click **Good Dynamics**.
6. In the drop-down list, click the name of the profile that you want to assign to the user.
7. If a Good Dynamics profile is already assigned directly to the user, click **Replace**. Otherwise, click **Assign**.

In BES12, assign an app group to a user account

Before you begin:

- In BES12, create an app group that contains all of the Good apps

1. In the BES12 management console, on the menu bar, click **Users**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **Apps** section, click +.
5. Select the check box beside the app group that you want to assign to the user account.
6. Click **Next**.
7. In the **Disposition** drop-down list for the app, perform one of the following actions:
   - To require users to install the apps, select **Required**.
   - To permit users to install and remove the apps, select **Optional**.
8. Click **Assign**.

In BES12, assign the activation profile to a user account

Before you begin:

- In BES12, create an activation profile.

1. In the BES12 management console, on the menu bar, click **Users**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the **IT policy and profiles** section, click +.
5. Click **Activation**.
6. In the drop-down list, click the activation profile that you created.
7. If an activation profile is already assigned directly to the user, click **Replace**. Otherwise, click **Assign**.

Activate an Android device

Send the following activation instructions to the device user.

1. On the device, install the BES12 Client. You can download the BES12 Client from Google Play.
2. On the device, tap **BES12 Client**.
3. Read the license agreement and tap **I Agree**.
4. Type your work email address and tap **Next**.
5. If necessary, type the server address and tap **Next**. You can find the server address in the activation email message you received or in BES12 Self-Service.
6. Confirm that the certificate details displayed on the device are accurate, and tap **Accept**. If your administrator sent you the certificate details separately, you can compare the information displayed with the information you received.
7. Type your activation password and tap **Activate My Device**.
8. Tap **Next**.
9. Depending on your security settings, you may be prompted to create a screen unlock option.
10. Tap **Activate**.
11. Good Dynamics will be configured on the device and, if your administrator has assigned you any apps, you will be prompted to install them.

Activate an iOS device

Send the following activation instructions to the device user.

1. On the device, install the Good for BES12 app. You can download Good for BES12 from the App Store.
2. On the device, tap **Good for BES12**.
3. Read the license agreement and tap **I Agree**.
4. Type your work email address and tap **Go**.
5. If necessary, type the server address and tap **Go**. You can find the server address in the activation email message you received or in BES12 Self-Service.
6. Confirm that the certificate details displayed on the device are accurate, and tap **Accept**. If your administrator sent you the certificate details separately, you can compare the information displayed with the information you received.
7. Type your activation password and tap **Activate My Device**.
8. Tap **Install** to install the required certificate.
9. Good Dynamics will be configured on the device. If you are prompted to enter the password for your email account or the passcode for your device, follow the instructions on the screen.
10. If your administrator has assigned you any apps, you will be prompted to install them.

Legal notice

2

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

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

Published in Canada