

Migration Guide

Good for Enterprise to BlackBerry Work



Contents

Good for Enterprise to BlackBerry Work transition guide.....	4
Key concepts.....	4
Installation requirements.....	5
Steps to transition from Good for Enterprise to BlackBerry Work.....	5
Create a BlackBerry Dynamics profile.....	6
BlackBerry Dynamics profile settings.....	6
Make BlackBerry Work available to users.....	11
Update the app list.....	11
Configure BlackBerry Work app settings.....	11
BlackBerry Work app configuration settings.....	12
Configure BlackBerry Work connection settings.....	22
Creating and managing user groups.....	23
Creating directory-linked groups.....	23
Create a local group.....	25
Assign the BlackBerry Dynamics profile to a user group.....	27
Assign an app to a user group.....	27
Connect Good Mobile Control to BlackBerry UEM.....	28
Steps to migrate users.....	29
Remove the GFE MDM profile on iOS devices.....	29
Migrate from Good for Enterprise to BlackBerry Work.....	30
Decommissioning Good for Enterprise.....	30
Legal notice.....	32

Good for Enterprise to BlackBerry Work transition guide

This document explains how to plan a transition from Good for Enterprise to BlackBerry Work.

Key concepts

Product	Description
BlackBerry Dynamics	With the exception of Good for Enterprise, all BlackBerry Dynamics apps now run on the BlackBerry Dynamics platform. ISV and custom enterprise apps are also built on the BlackBerry Dynamics platform.
BlackBerry Enterprise Mobility Server	BlackBerry Enterprise Mobility Server is an application middleware server platform that provides various mobile backend services (MBaaS) from enterprise backends such as Microsoft Exchange, Microsoft Lync, and Microsoft SharePoint. These services are used by BlackBerry Work, other BlackBerry Dynamics apps, and ISV apps built with the BlackBerry Dynamics SDK. The BlackBerry Enterprise Mobility Server delivers these as standardized backend services around push notifications, directory lookups, online presence, and more.
BlackBerry UEM	<p>BlackBerry UEM is a multiplatform EMM solution that provides comprehensive device, app, and content management with integrated security and connectivity. With BlackBerry UEM you can:</p> <ul style="list-style-type: none"> • Manage BlackBerry 10, iOS, OS X, Android (including devices that use Samsung KNOX), Windows (including Windows 10 tablets and computers), and BlackBerry OS (version 5.0 to 7.1) devices • Use a simple web-based interface to manage BYOD, COPE, and COBO devices and protect business information • Manage complex fleets of devices using comprehensive reporting and dashboards, dynamic filters, and robust search capabilities • Keep mobile workers connected with the information that they need

Installation requirements

Refer to the requirements for the environment that you are installing.

Product	Description
BlackBerry UEM 12.7 Maintenance Release 1 or later	See the BlackBerry UEM Planning content and the BlackBerry UEM Installation and Upgrade content .
BlackBerry Enterprise Mobility Server	Your environment may require the advanced services that a BlackBerry Enterprise Mobility Server installation provides to BlackBerry Work and other BlackBerry Dynamics apps. For example, you may require Push Registration, BlackBerry Presence, BlackBerry Directory Lookup, and BlackBerry Docs. For comprehensive guidance on installing BlackBerry Enterprise Mobility Server and deploying the services necessary to support BlackBerry Work and any other BlackBerry Dynamics apps that you intend to deploy, see the BlackBerry Enterprise Mobility Server Installation and Configuration content .

Steps to transition from Good for Enterprise to BlackBerry Work

Step	Action
1	Install BlackBerry UEM.
2	Install the BlackBerry Enterprise Mobility Server.
3	Create a BlackBerry Dynamics profile or update the Default BlackBerry Dynamics profile.
4	Make BlackBerry Work available to users.
5	Configure BlackBerry Work app settings
6	Configure BlackBerry Work connection settings
7	Create a user group and assign the following to it:

Step	Action
	<ul style="list-style-type: none"> BlackBerry Dynamics profile BlackBerry Work and any other apps that you want to assign to users
8	Connect Good Mobile Control to BlackBerry UEM.
9	Instruct users to activate their devices, install BlackBerry Work, and remove Good for Enterprise.
10	Decommission Good for Enterprise.

Create a BlackBerry Dynamics profile

- On the menu bar, click **Policies and Profiles**.
- Click **Policy > BlackBerry Dynamics**
- Click **+**.
- Type a name and description for the profile.
- Configure the appropriate values for the profile settings. For more information about each profile setting, see [BlackBerry Dynamics profile settings](#).
- Click **Add**.

After you finish: If necessary, [rank profiles](#).

BlackBerry Dynamics profile settings

BlackBerry Dynamics profiles are supported on the following device types:

- iOS
- Android
- macOS
- Windows

BlackBerry Dynamics profile setting	Description
Configuration	

BlackBerry Dynamics profile setting	Description
Require device management to use BlackBerry Dynamics apps	This setting specifies whether a device must be activated with MDM to use BlackBerry Dynamics apps.
Enable UEM Client to enroll in BlackBerry Dynamics	If a device is using the BlackBerry UEM Client, this setting specifies whether the BlackBerry Dynamics manages the activation of BlackBerry Dynamics apps and whether BlackBerry Dynamics apps can be used on the device. If this option is not selected, BlackBerry Dynamics apps could be removed from the device because the device will not be enabled for BlackBerry Dynamics. If you do not plan to use BlackBerry Dynamics in your environment, do not select this setting.
Password	
Password expiration	This setting specifies whether the password for a BlackBerry Dynamics app expires and the number of days a password remains valid before it expires.
Do not allow previous passwords	This setting specifies whether previous passwords can be used and the maximum number of previous passwords that cannot be used for a BlackBerry Dynamics app.
Minimum password length	This setting specifies the minimum length of the password for a BlackBerry Dynamics app.
Allowed occurrences of a character	This setting specifies how many times a character can appear in a password for a BlackBerry Dynamics app.
Require both letters and numbers	This setting specifies whether the password must contain both letters and numbers for a BlackBerry Dynamics app.
Require both uppercase and lowercase	This setting specifies whether the password must contain both uppercase and lowercase letters for a BlackBerry Dynamics app.
Require at least one special character	This setting specifies whether the password must contain at least one special character for a BlackBerry Dynamics app.
Do not allow sequences of more than two numbers	This setting specifies whether the password can contain more than two sequential numbers (for example, 1, 2, 3) for a BlackBerry Dynamics app.
Do not allow more than one password change per day	This setting specifies whether a password can be changed more than once every 24 hours for a BlackBerry Dynamics app.
Do not allow personal information	This setting specifies whether the following personal information can be used in a password for a BlackBerry Dynamics app: <ul style="list-style-type: none"> The user's first and last names (excluding initials) as recorded in Active Directory

BlackBerry Dynamics profile setting	Description
	<ul style="list-style-type: none"> The part of an email address before the @ sign.
Allow Biometrics	<p>This setting specifies whether BlackBerry Dynamics apps can be unlocked using biometric input when they are already open in the app switcher on iOS devices. You can allow the following options:</p> <ul style="list-style-type: none"> None Allow Touch ID Allow Face ID Allow Touch ID and Face ID
Enable Touch ID and Face ID from cold start	<p>This setting specifies whether BlackBerry Dynamics apps can be unlocked using the selected biometric input methods when they are opened for the first time after a device restarts.</p>
Require password to be re-entered and disable Touch ID and Face ID	<p>This setting specifies a period of time after which users must enter a password to unlock a BlackBerry Dynamics app and re-enable Touch ID, Face ID, or both.</p>
Allow Android fingerprint authentication	<p>This setting specifies whether BlackBerry Dynamics apps can be unlocked using Android fingerprint authentication.</p>
Do not require password	<p>These settings specify whether a user can access a BlackBerry Dynamics app without entering a password. The choices are:</p> <ul style="list-style-type: none"> iOS macOS Android Windows
Blocked password list	
Blocked password file (.txt)	<p>This setting specifies a list of banned passwords. You can download the previously uploaded list of banned passwords. Passwords in the list must meet the following requirements: each password must be separated by a hard return, only UTF-8 characters are supported, and passwords must be 14 characters or less.</p>
Lock screen	
Require password when BlackBerry Dynamics apps start	<p>This setting specifies whether a password is required each time a BlackBerry Dynamics app is started.</p> <p>Note: If you are using authentication delegation, do not select this option.</p>

BlackBerry Dynamics profile setting	Description
Require password after period of inactivity	This setting specifies the period of inactivity that must elapse before a password is required.
Take action after invalid password attempts	<p>This setting specifies whether there is a limit to the number of times that a user can enter an incorrect password. If you select this rule, specify the number of times that a user can enter an incorrect password and the action that occurs after the limit has been reached. Choose one of the following actions:</p> <ul style="list-style-type: none"> • Lock out user • Wipe Data
Wearables	
Allow wearables	This setting specifies whether BlackBerry Dynamics apps can be used on a wearable device. If you select this rule, specify the how much time must elapse before the wearable device is disconnected and whether the wearable can reconnect automatically.
App authentication delegation	
<p>You can select up to three apps to act as the authentication delegate on behalf of other apps so that users do not have to create a password for each BlackBerry Dynamics app that they install. After an authentication delegate is configured, each time a user opens a BlackBerry Dynamics app, the device displays the password screen for the authentication delegate instead of the app that they are attempting to open. After the user enters the password for the authentication delegate, the user can open the BlackBerry Dynamics app.</p>	
<p>You can choose any app to be the authentication delegate for other apps, but it is recommended that you choose your most commonly used app to be the primary authentication delegate to provide the most seamless experience for the user.</p>	
Data leakage prevention	
Do not allow copying data from non BlackBerry Dynamics apps into BlackBerry Dynamics apps	This setting specifies whether users can copy data from non BlackBerry Dynamics apps to BlackBerry Dynamics apps.
Do not allow Android dictation	This setting specifies whether Android device users can use voice dictation with BlackBerry Dynamics apps.
Do not allow screen captures on Android devices	This setting specifies whether Android device users can take screen captures in BlackBerry Dynamics apps.

BlackBerry Dynamics profile setting	Description
Do not allow screen recording and sharing on iOS devices	<p>This setting specifies whether iOS device users can share and record screens in BlackBerry Dynamics apps.</p> <p>This setting applies to devices running iOS 11 and later.</p>
Do not allow iOS dictation	<p>This setting specifies whether iOS device users can use voice dictation with BlackBerry Dynamics apps.</p>
Do not allow custom keyboards on iOS devices	<p>This setting specifies whether iOS device users can use custom keyboards with BlackBerry Dynamics apps.</p>
Enable FIPS	<p>This setting specifies whether compliance with U.S. Federal Information Processing standard 140-2 is enforced.</p>
Certificates	
Enable device certificate store	<p>This setting specifies whether BlackBerry Dynamics apps can get certificates from the device certificate store.</p>
Detailed logging	
Enable detailed logging for BlackBerry Dynamics apps	<p>This setting specifies whether log files can be generated and uploaded from BlackBerry Dynamics apps.</p>
Prevent users from turning on detailed logging in BlackBerry Dynamics apps	<p>This setting specifies whether users can turn on the ability to generate and share detailed log files from BlackBerry Dynamics apps.</p>
Agreement	
Enable an agreement message for BlackBerry Dynamics apps	<p>This setting specifies whether to display a message in BlackBerry Dynamics apps that the user must acknowledge. If authentication delegation is enabled, the message is displayed only in the authenticator app. If you select this rule, complete the following actions:</p> <ul style="list-style-type: none"> • Specify if the message is displayed each time the app is unlocked, otherwise the message is only displayed the first time the user opens the app. • In the Message field, create the message that you want to display. <p>Note: On Android devices, only the first 4000 characters are displayed.</p>

Make BlackBerry Work available to users

To manage BlackBerry Work in BlackBerry UEM, you must add BlackBerry Work to the app list. To add BlackBerry Work to the app list in BlackBerry UEM, your organization must be entitled to use BlackBerry Work in the BlackBerry Marketplace for Enterprise Software. After your organization is entitled to use the app, you can update the app list to synchronize BlackBerry Work with BlackBerry UEM right away or wait until it synchronizes automatically. BlackBerry UEM synchronizes BlackBerry Dynamics apps every 24 hours. After the apps have been added to the app list, they can be assigned to users.


For a complete description of how to manage BlackBerry Dynamics apps in BlackBerry UEM, see [Managing BlackBerry Dynamics apps](#).

1. Log in to your account at <https://apps.good.com/pce/#/apps>.
2. Locate the app in the BlackBerry Marketplace for Enterprise Software and request a trial. The app will be made available to your organization and can be assigned to users after the app has been synchronized to BlackBerry UEM.
3. To purchase the app, contact your sales representative or your channel partner sales representative.

After you finish:

- [Update the app list](#).
- To allow users to install and activate BlackBerry Work on their devices, [assign BlackBerry Work to a user group](#).

Update the app list

1. On the menu bar, click **Apps**.
2. Click .

Configure BlackBerry Work app settings

You must add your Exchange ActiveSync server information and, optionally, configure other settings.

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Work app.
3. On the BlackBerry Dynamics tab, in the App configuration table, click +.
4. Type a name for the app configuration.
5. On the **Exchange Settings** tab, under **Exchange ActiveSync Settings** configure the following settings:
 - a. In the **Default Domain** field, specify the default Windows NT Domain that BlackBerry Work will automatically attempt to connect to when users log in to BlackBerry Work. If your server uses the newer UPN (email@host.com) style login instead of the older (domain\user) style login, leave this field blank.

- b. In the **Active Sync Server** field, specify the default Exchange ActiveSync server that BlackBerry Work will attempt to connect to when users log in to BlackBerry Work (for example, cas.mydomain.com).
 - c. In the **Auto Discover URL** field, specify the auto discover URL if known. This will speed up the auto discover setup process (for example, https://autodiscover.mydomain.com).
 - d. In the **Auto Discover Connection Timeout in Seconds (iOS only)** field, specify the auto discover connection timeout in seconds.
6. Optionally, configure any other settings. See [BlackBerry Work app configuration settings](#) for a description of all of the settings that you can configure.
 7. Click **Save**.

BlackBerry Work app configuration settings

App Settings tab	Description
Autodiscover	<p>If you select this option, BlackBerry Work automatically discovers the Exchange ActiveSync server.</p> <p>Note: Due to possible security vulnerabilities, it is not recommended that you select this option.</p>
Authorized Email Domains	<p>Select the "Display warning while sending message if the number of unauthorized recipient email domain(s) is" option if you want to display a warning message to users that attempt to send a message to the number of unauthorized domains specified in the drop-down list.</p> <p>Select the "Display warning for received messages if the sender's email domain is unauthorized" option if you want to display a warning to users when they receive messages from senders that are not listed in the Authorized email domains list.</p> <p>If you select either of the options above, specify a list of authorized email domains. Use a comma separated list, with no spaces, to specify authorized email domains. You can edit the sample text displayed in the warning message field.</p>
External Email Marking	<p>If you select this option, subject lines of email messages sent outside of the user's domain are prepended with the text specified in the Text to prepend field.</p>
Avatar Photos	<p>If you select this option, contact photographs are displayed in BlackBerry Work. If this option is not selected, the user's initials are displayed instead of a photograph.</p>
Presence Service	<p>If you select this option, users can see the online status of their Microsoft Lync contacts.</p>

App Settings tab	Description
Email Search	If you select this option, users can search email messages on the server.
Diagnostics	If you select this option, users can perform app diagnostics from the BlackBerry Dynamics Launcher on their devices.
BlackBerry Gatekeeping Service	If you select this option, unauthorized devices are prevented from using Exchange ActiveSync unless they are explicitly added to the allowed list using the BlackBerry Gatekeeping Service. To use the BlackBerry Gatekeeping Service, you must create a gatekeeping configuration for the Microsoft Exchange Server or Microsoft Office 365 and assign an email profile to users that has the automatic gatekeeping server selected. For details on how to configure the BlackBerry Gatekeeping Service, see Controlling which devices can access Exchange ActiveSync .
Notifications tab	Description
Select level of detail in Email notifications	Select the level of detail that users see in email notifications.
Select level of detail in Calendar notifications	<p>Select the level of detail that users see in calendar notifications.</p> <p>Select the Show only generic notifications when app is locked (Android only) option to show only generic information in notifications if the app is locked.</p> <p>Select the Show notifications on connected wearable devices (Android Wear only) option to display notifications on Android Wear devices.</p> <p>Select the Show Work Calendar lock-screen widget (iOS only) options to allow the work calendar widget to be accessed from the lock screen of iOS 10 and later devices.</p>
Additional options for notifications on Android Wear devices	Select whether there are additional notifications for Android Wear devices.
iOS App Icon Badge	Select this option to allow users to choose between displaying a badge count for unread and new email messages as their default badge count on the app icon. If this option is not selected, the app icon badge will reflect the number of new email messages that were received since the user last closed the app, and the user cannot select “Unread Mails” as a badge count preference.
S/MIME tab	Description
Enhanced Security	Select the Periodically require PIN entry to access SMIME capabilities option if you want users to be required to periodically enter a PIN to use S/MIME.

S/MIME tab	Description
Sending	<p>In the Default signing algorithm drop-down list, select the algorithm to use for signing sent messages.</p> <p>In the Default encryption algorithm, select the encryption algorithm to use.</p> <p>Select whether emails must be signed and encrypted.</p>
Receiving	<p>In the Automatically download the body of S/MIME emails drop-down list, select how the body of S/MIME email messages is downloaded. Wi-Fi is supported on Android devices only. If you select this option, iOS devices are set to "Never."</p> <p>Select the Perform name checking (verify email address in certificate matches user's account) option to perform name checking. Name checking verifies that the email address in the certificate matches user's account.</p>
Certificate Management	Specify when to clear the public certificate cache.
Revocation Checking when the OCSP server is available	<p>Select the Enable revocation checking option to enable revocation checks and specify the depth of certificate checking.</p> <p>Select the Use AIA extension in certificate if present option to use the AIA extension in certificates if present.</p> <p>In the Default OCSP URL field, specify the default OCSP URL to use if the AIA extension cannot be used or it is not present in a certificate.</p>

Address Book tab	Description
Address Book Sync	<p>Select the Allow syncing BlackBerry Contacts to device option to synchronize contacts to devices and choose the fields that are synchronized.</p> <p>In the Maximum length for notes field field, specify the maximum length for the notes field.</p> <p>Select the Even if iCloud is enabled, allow syncing BlackBerry Contacts to device option to allow synchronization to occur when iCloud is enabled.</p>
Caller ID	Select the Allow device to use BlackBerry Contacts option if you want to allow BlackBerry Work to access the user's BlackBerry Work contact list to display contact name for incoming and outgoing phone calls.
GAL Search	Specify the maximum number of results to display when searching the global address list (GAL).
Recipients	Specify whether caching is enabled. When caching is enabled, the cache is used to offer autocomplete suggestions for recipients during email composition.

Interoperability	Description
Camera and Device Photo Gallery permissions	Specify whether to allow access to the device camera, the photo gallery, or both.
Voice	Specify whether to allow users to use the native phone app on a device or VOIP apps.
SMS	Specify whether to allow users to initiate their native SMS apps by tapping the SMS icon or whether they must use BlackBerry Dynamics SMS apps.
Misc	Specify whether to allow access to the user's native browser or native map app.
Launch 3rd Party App (iOS only)	<p>Specify whether to enable two-factor authentication integration with a third-party RSA SecurID app using a CTF token seed.</p> <p>Note: BlackBerry Work supports CTF-based and file-based provisioning using BlackBerry Access, as well as CTF-based provisioning using a native RSA SecurID app. For more information about configuring RSA soft-token authentication and provisioning the token seed record your organization sends to users, see the BlackBerry Access Administration Guide.</p>
Launch 3rd Party App Universal link (iOS only, BETA)	<p>Universal links allow iOS users to be automatically redirected to an installed app without going through Safari when they click links in a website. If the app isn't installed on the device, the link opens the website in Safari.</p> <p>You can specify a list of universal links that users can open from BlackBerry Work for iOS. If you add a universal link to this list, the link will redirect to the appropriate app if it is installed on a user's device. If a user clicks on a universal link that is not added to this list, the link will not be redirected to an app and will open in Safari, even if the app is installed on a user's device.</p> <p>To add multiple URLs, insert a carriage return between each URL that you want to add.</p>
Allow 3rd Party App to Send Mail	Specify whether email messages can be sent using mailto:/gmmmailto:/gwmmailto
File Transfer Privileges	Specify whether to allow the transfer of files to third-party native apps on the user's device. You can allow and disallow specific apps by app ID.
Skype for Business	<p>If you are currently using Skype for Business 2015 or later in your environment, you can allow users to add meetings and join meetings directly from their calendars.</p> <p>Select the Allow to create Skype For Business meetings in calendar option to allow users to add Skype for Business meetings to their calendars.</p> <p>Select the Allow launching into Skype for Business app on mobile option to allow users to make voice and video calls and to be able to join Skype for Business</p>

Interoperability	Description
	<p>meetings directly from a calendar invitation. The meeting is automatically opened in the Skype for Business client and users must have the Skype for Business client installed on their devices.</p> <p>In the Domain of Skype for Business meeting link field, enter the fully qualified domain name of the Skype for Business meeting links to allow internal users to use the Join meeting button in event details. By entering this domain name, BlackBerry Work knows which domain to use if links are created by users in a different domain in Microsoft Outlook or the Outlook Web App.</p>

Docs and Attachments tab	Description
Docs Repository	Specify whether to enable a file repository on the device, local or server docs repositories, and Box, and whether to force users to save pending uploads. Note: By default users are alerted about any pending uploads every 24 hours. If Forced Pending Uploads Policy is selected, users are blocked from taking any document related actions in BlackBerry Work until all files are successfully uploaded to the server.
Sending Attachments	Specify whether to allow outgoing attachments and specify the maximum size and the file extensions that are allowed or disallowed.
Receiving/Opening Attachments	Specify whether to allow incoming attachments and specify a maximum size and the file extensions that are allowed or disallowed.

Classification tab	Description
Email classification	Specify whether to enable email classification markings, such as INTERNAL, CONFIDENTIAL, NO FORWARD, and/or NO REPLY. To edit the XML classes, highlight and delete the code that you want to remove.

Basic Configuration tab	Description
Security Settings	<p>Select Disable SSL Certificate Checking to disable SSL certificate verification for ActiveSync/Microsoft Exchange Web Services in test and POC environments.</p> <p>Select Expect Kerberos Constrained Delegation and suppress username/password entry for Exchange to specify whether Kerberos Constrained Delegation will be used for logging in to Microsoft Exchange. If this option is not selected, NTLM/Basic authentication will be used.</p>

Basic Configuration tab	Description
	<p>Select Clients must have individual login certificates (SSL) uploaded in the GC to specify whether clients must have individual login certificates (SSL) uploaded to the BlackBerry UEM management console. These certificates are used for login instead of basic credentials (username/password).</p>
Enterprise Server Settings	<p>In the Server List Reshuffle Period (minutes) field, specify the frequency that the server list, if present, is reshuffled for load balancing purposes.</p> <p>In the Server List Quarantine Period (minutes) field, specify how long BlackBerry Work waits before retrying if BlackBerry UEM is not working.</p>
Client Settings	<p>In the Sync Email Body Size (Kb) field, specify the size, in KB, of the partial message body downloaded from the server if the user selects the option to download partial message content.</p> <p>Select the Use BEMS to perform AutoDiscover of the EAS/EWS endpoint for the user option to specify that the client will use the BlackBerry Server Autodiscover service to determine the EAS/EWS endpoint for the user.</p> <p>Select the Create and consume rights-managed email messages option to specify that IRM must be enabled for user mailboxes on Microsoft Exchange.</p>
Other Settings	<p>In the Send Feedback Email Address field, specify the email address where client feedback email messages are sent. Add multiple comma delimited recipients as needed.</p> <p>In the Report Phishing Email Address field, specify whether users can report emails as phishing. The reported emails are forwarded to the email address provided in this field then moved to Trash folder.</p>
Account Setup	<p>When Skip Email Short Form Setup Active Directory is selected, users must input their Microsoft Active Directory usernames, passwords, and domains during device activation.</p>
ActiveSync and Auto Discover Authentication Methods (iOS Only)	<p>Specify the authentication methods to use. If only certain authentication methods are supported from Microsoft Exchange, set those values to minimize the user setup time. (For example, if Auto Discover and ActiveSync IIS Auth Settings are set to allow only NTLM and Basic, then de-select Negotiate in above app setting.) If none are selected, the default Microsoft Exchange setting is used. If using client-based authentication, check none of the options.</p>
Exchange Web Services Authentication Methods (iOS Only)	<p>Specify the authentication methods to use. If only certain authentication methods are supported from Microsoft Exchange, set those values to minimize the user setup time. (For example, if EWS IIS Auth Setting is set to allow only NTLM, then select only NTLM above for an optimal setup experience.) If none are selected</p>

Basic Configuration tab	Description
	above, the default Microsoft Exchange setting is used. If using client-based authentication, check none of the options.
Exchange Web Services Settings	Specify the Microsoft Exchange Web Services URL endpoint (for example, https://mydomain.com/EWS/Exchange.asmx).
Exchange ActiveSync Settings	<p>In the Default Domain field, specify the Windows NT Domain to try automatically when logging in. If your server uses newer UPN (email@host.com) style login instead of the older (domain\user) style login, this field should be left blank.</p> <p>In the ActiveSync Server field, specify the default Microsoft Exchange Server to connect to (for example, cas.mydomain.com).</p> <p>In the Autodiscover URL field, specify the auto discover URL if known. This speeds up the auto discover setup process (for example, https://autodiscover.mydomain.com).</p> <p>In the Autodiscover Connection Timeout in Seconds (iOS only) field, specify the timeout setting for iOS devices.</p>
Advanced Settings	Specify additional configuration parameters in this text area. Contact BlackBerry Support for more details.

Advanced Settings tab	Description
ActiveSync User Name Formats (iOS Only)	<p>Select the username formats that can be used to authenticate with your Exchange ActiveSync server. To simplify user setup time, select only the username formats that are supported by your Exchange ActiveSync server.</p> <p>If you do not select an option, all options are allowed.</p>
Exchange Web Services User Name Formats (iOS Only)	<p>Select the username formats that can be used to authenticate with Microsoft Exchange Web Services.</p> <p>To simplify user setup, select only the username formats that are supported by Microsoft Exchange Web Services.</p> <p>If you do not select an option, all options are allowed.</p>
Exchange TLS Certificate Settings	<p>Specify the user credential profile that contains the TLS certificate to be used to connect to Microsoft Exchange. The name of the profile that you specify here must match the name of the user credential profile that was created in the BlackBerry UEM management console.</p> <p>For more information on user credential profiles, see Using user credential profiles to send certificates to devices.</p>

Advanced Settings tab	Description
Email Sync Window	<p>Specify the number of days in the past to synchronize email messages to devices. If the setting on a device allows for more days than the server setting, the server setting is used and email messages that are older than the server setting are removed from the device. If the setting on the device allows fewer days than the server setting, the setting on the device remains the same. The user can change the setting on the device to fewer days than the server setting.</p>
Exchange ActiveSync 16.0 Protocol	<p>If supported by your Microsoft Exchange server, specify whether to use Exchange ActiveSync version 16 for synchronization between Microsoft Exchange and BlackBerry Dynamics apps.</p> <p>Note: This setting must be enabled if you want to allow users to be able to synchronize their Drafts folder to BlackBerry Work. For more information on how to synchronize the Drafts folder, see KB50339 Synchronizing draft messages in BlackBerry Work 2.12 and later.</p>
Shared Mailboxes	<p>Select the Enable access to Shared Mailboxes option if you want to allow users to add a shared mailbox that they are a delegate for in BlackBerry Work. If this option is disabled after shared mailboxes have been added, existing shared mailboxes are removed, and they are not restored if the setting is enabled again. Also, if a user attempts to add a shared mailbox when this option is disabled, they will not be able to add the mailbox and will see a message in the BlackBerry Work app stating that they must contact their administrator.</p>
Office 365 Settings	<p>Select the Use Office 365 Settings option to configure options for Microsoft Office 365. If selected, specify the following:</p> <ul style="list-style-type: none"> • Select the Use Office 365 Modern Authentication option to use modern authentication instead of basic authentication. Modern authentication enables BlackBerry Work to use sign-in features such as Multi-Factor Authentication, SAML-based third-party Identity Providers, and smart card and certificate-based authentication. • In the Azure App ID field, specify the Microsoft Azure app ID for BlackBerry Work. For information on how obtain an Azure ID, see Obtain an Azure app ID for BlackBerry Work. • In the Office 365 Sign On URL field, specify the web address that BlackBerry Work should use when signing in to Office 365. If you do not specify a value, BlackBerry Work will use <code>https://login.microsoftonline.com</code> during setup. • In the Office 365 Tenant ID field, specify the tenant ID of Office 365 server that you want BlackBerry Work to connect to during setup. If you do not specify a value, a value of "common" is used.

Advanced Settings tab	Description
	<ul style="list-style-type: none"> In the Office 365 Resource field, specify the URL of the Microsoft Exchange Online server. In the Redirect URI field, specify the URI that you entered in the Microsoft Azure portal. Select the Proxy Office 365 Modern Authentication requests (Android only) setting to force all Office 365 Modern Authentication requests to go through the BlackBerry Proxy instead of connecting directly to the Internet.
Performance Reporting tab	Description
Enable Performance Reporting	Specify whether to monitor performance of the BlackBerry Work app.
HTTP Connection Error	Specify whether to report HTTP connection errors between BlackBerry Work and the specified application servers.
HTTP Response Time	Specify whether to report HTTP responses that are taking longer than the specified time. Enter the application server addresses to monitor.
HTTP Status Code	Specify whether to report a specified HTTP status code. Enter the application server addresses to monitor.
Don't send reports for duration (in seconds)	Specify the amount of time to wait before sending another report.

Obtain an Azure app ID for BlackBerry Work

If you are configuring Office 365 settings in the app configuration for BlackBerry Work, you may need to obtain and copy the Azure app ID for BlackBerry Work.

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New application registration**.
5. In the **Name** field, enter a name for the application. This is the name that users will see.
6. In the **Application type** drop-down list, select **Native**.
7. In the **Redirect URI** field, enter the following:

- **com.blackberry.work://connect/o365/redirect**

8. Click **Create**.
9. After the app has been created, in the toolbar under the name of the app, click **Settings**.
10. Under API Access, click **Required permissions**.
11. Click **Add**.
12. Click **Select an API**
13. Select **Office 365 Exchange Online (Microsoft.Exchange)**.
14. Click **Select**.
15. Select the following permission for Office 365 Exchange Online (Microsoft.Exchange)
 - **Access mailboxes as the signed-in user via Exchange Web Services**
16. Click **Select**.
17. Click **Done**.
18. Click **Add**.
19. Click **Select an API**
20. Click **Microsoft Graph**.
21. Click **Select**.
22. Select the following permissions for Microsoft Graph:
 - **Sign in and read user profile**
 - **Send mail as a user**
23. Click **Select**.
24. Click **Done**.
25. Click **Windows Azure Active Directory**.
26. If it is not already selected, select **Sign in and read user profile** and then click **Save** if you changed the value.
27. Click **Grant Permissions** to apply the permissions for the app. These settings will not be applied to the app until you have granted the updated permissions.
28. Click **Yes**.

You can now copy the Application ID for the app that you created. It is located under the name of the app, in the Application ID field.

Configure BlackBerry Work connection settings

When you configure your environment for BlackBerry Work, you must add the necessary Exchange ActiveSync servers and BlackBerry Enterprise Mobility Server instances to the connectivity profiles that you have assigned to users that will install BlackBerry Work.

1. On the menu bar, click **Policies and Profiles > Networks and Connections**.
2. Click **+** beside **BlackBerry Dynamics Connectivity profile** to create a new connectivity profile or click on the Default connectivity profile to edit it.
3. In the Additional servers section, click **+**.
4. In the **Server** field, specify the FQDN of the Exchange ActiveSync server.
5. In the **Port** field, specify the port for the Exchange ActiveSync server. By default, the port number is 443.
6. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
7. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
8. Click **Save**.
9. In the Additional servers section, click **+**.
10. In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
11. In the **Port** field, specify the port for the BlackBerry Enterprise Mobility Server. By default, the port number is 8080 or 8443.
12. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
13. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
14. Click **Save**.
15. In the App servers section, click **Add**.
16. Search for and select BlackBerry Work.
17. Click **Save**.
18. In the table for the app, click **+**.
19. In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
20. In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access the BlackBerry Enterprise Mobility Server.

21. In the **Priority** drop-down list, specify the priority of the BlackBerry Proxy cluster that must be used to reach the domain.
22. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
23. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
24. Click **Save**.
25. Click **Add** or **Save**.

Creating and managing user groups

A user group is a collection of related users who share common properties. Administering users as a group is more efficient than administering individual users because properties can be added, changed, or removed for all members of the group at the same time.

Users can belong to more than one group at a time. You can assign an IT policy, profiles, and apps in the management console when you create or update the settings for a user group. If the BlackBerry UEM domain supports BlackBerry OS (version 5.0 to 7.1) devices, you can also assign a BlackBerry OS IT policy, profiles, and software configurations.

You can create two types of user groups:

- Directory-linked groups link to groups in your company directory. Only directory user accounts can be members of a directory-linked group.
- Local groups are created and maintained in BlackBerry UEM and can have local user accounts and directory user accounts assigned to them.

After you create user groups, you can define a group as a member of another group. When you nest a group within a user group, members of the nested group inherit the properties of the user group. You create and maintain the nesting structure in BlackBerry UEM and you can nest both directory-linked groups and local groups within each type of user group.

Creating directory-linked groups

You can create groups in BlackBerry UEM that are linked to one or more groups in your company directory. These BlackBerry UEM groups are called "directory-linked groups." Only directory user accounts can be members of a directory-linked group.

At a scheduled interval, BlackBerry UEM automatically synchronizes the membership of a directory-linked group with its associated company directory group (or groups). Users that were added or removed from the company directory group are added or removed from the directory-linked group.

Note: When users are moved into a company directory group that is linked to a directory-linked group, they are assigned the policies, profiles, and apps that are assigned to the group. When users are removed from a company directory group that is linked to a directory-linked group, the policies, profiles, and app are removed from the user.






Each directory-linked group can link to only a single company directory. For example, if BlackBerry UEM has two Microsoft Active Directory connections (A and B), and you create a directory-linked group that is linked to connection A, you can link only to directory groups from connection A. You must create new directory linked groups for any other directory connections.

To enable this feature, [see "Enable directory-linked groups" in the Configuration content.](#)[see "Enable directory-linked groups" in the Configuration content.](#)

Synchronizing directory-linked groups does not add or delete users in BlackBerry UEM. To allow BlackBerry UEM to create user accounts when new company directory users are created, you must enable and configure onboarding. For more information, [see "Enabling onboarding" in the Configuration content.](#)[see "Enable onboarding" in the Configuration content.](#)


Create a directory-linked group

Before you begin: Enable directory-linked groups. For instructions, [see the Configuration content.](#)[see the Configuration content.](#)

1. On the menu bar, click **Groups**.
2. Click .
3. Type the group name.
4. In the **Linked directory groups** section, perform the following actions:
 - a. Click .
 - b. Type the name or partial name of the company directory group you want to link to.
 - c. If you have more than one company directory connection, select the connection that you want to search. After you have made this selection, the directory-linked group is permanently associated with the selected connection.
 - d. Click .
 - e. Select the company directory group in the search results list.
 - f. Click **Add**. The company directory group displays in the list and the company directory connection the group is linked to displays beside the section title.
 - g. If necessary, select the **Link nested groups** check box. You can leave the check box unselected to link to all nested groups, or you can select the check box to allow the directory settings to control the number of nested groups.
 - h. Repeat these steps to link additional groups.
5. To assign a user role to the directory-linked group, perform the following actions:
 - a. In the **User role** section, click .
 - b. In the drop-down list, click the name of the user role that you want to assign to the group.
 - c. Click **Add**.
6. To assign an IT policy or profile to the directory-linked group, perform the following actions:
 - a. In the **IT policy and profiles** section, click .


- b. Click **IT policy** or a profile type.
 - c. In the drop-down list, click the name of the IT policy or profile that you want to assign to the group.
 - d. Click **Assign**.
7. To assign an app to the directory-linked group, in the **Assigned apps** section, click **+**.
 8. Search for the app.
 9. In the search results, select the app.
 10. Click **Next**.
 11. In the **Disposition** drop-down list for the app, perform one of the following actions:
 - To install the app automatically on devices, and to prevent users from removing the app, select **Required**. This option is not available for BlackBerry apps.
 - To permit users to install and remove the app, select **Optional**.
 12. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
 13. Click **Assign**.
 14. Click **Add**.

Add a company directory group to an existing directory-linked group

1. On the menu bar, click **Groups**.
2. Click the directory-linked group.
3. Click the **Settings** tab.
4. Click .
5. In the **Linked directory groups** section, click **+**.
6. Type the company directory group name.
7. Click **Search**.
8. Select the company directory group in the search results list.
9. Click **Add**.
10. If required, select **Link nested groups**.

Create a local group

1. On the menu bar, click **Groups**.

2. Click .
3. Type a name for the user group.
4. Optionally, type a description for the user group.
5. To assign a user role to the local group, perform the following actions:
 - a. In the **User role** section, click **+**.
 - b. In the drop-down list, click the name of the user role that you want to assign to the group.
 - c. Click **Add**.
6. To assign an IT policy or profile to the local group, perform the following actions:
 - a. In the **IT policy and profiles** section, click **+**.
 - b. Click **IT policy** or a profile type.
 - c. In the drop-down list, click the name of the IT policy or profile that you want to assign to the group.
 - d. Click **Assign**.
7. To assign an app to the user group, in the **Assigned apps** section, click **+**.
8. Search for the app.
9. In the search results, select the app.
10. Click **Next**.
11. In the **Disposition** drop-down list for the app, perform one of the following actions:
 - To install the app automatically on devices, and to prevent users from removing the app, select **Required**. This option is not available for BlackBerry apps.
 - To permit users to install and remove the app, select **Optional**.

Note: If the same app is assigned to a user account and to the user group that the user belongs to, the disposition of the app assigned to the user account takes precedence.
12. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
13. Click **Assign**.
14. When you are finished specifying the user group properties, click **Add**.

Assign the BlackBerry Dynamics profile to a user group

Before you begin: [Create a BlackBerry Dynamics profile.](#)

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

Assign an app to a user group

When you assign apps to a user group, the apps are made available to any applicable devices that the members of the user group have activated. You can also assign apps to user groups for device types that the members of the user group have not activated yet. This makes sure that if any member of the group activates a different device type in the future, the proper apps are made available to new devices.

If a user account is a member of multiple user groups that have the same apps or app groups assigned to them, only one instance of the app or app group appears in the list of assigned apps for that user account. The same app can be assigned directly to the user account, or inherited from user groups or device groups. The settings for the app (for example, whether the app is required) are assigned based on priority. Device groups have the highest priority, then user accounts, then user groups.

Before you begin:

- Add the app to the available app list.
 - Optionally, add the apps to an app group.
1. On the menu bar, click **Groups > User**.
 2. In the group list, click the name of the user group.
 3. In the **Assigned apps** section, click **+**.
 4. In the search field, type the app name, vendor, or URL of the app that you want to add.
 5. Select the check box beside the apps or app group that you want to assign to the user group.
 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 app, select **Required**.
 - To permit users to install and remove the app, select **Optional**.

Note: If the same app is assigned to a user account, a user group that the user belongs to, and the device group the device belongs to, the disposition of the app assigned in the device group takes precedence.
8. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
9. For iOS and Android devices, if there is an available app configuration, select the app configuration to assign to the app.
10. Perform one of the following tasks:

Task	Steps
If you have not added a VPP account or you are not adding an iOS app	<ol style="list-style-type: none"> 1. Click Assign.
If you are adding an iOS app and you have added at least one VPP account	<ol style="list-style-type: none"> 1. Click Next. 2. Select Yes if you want to assign a license to the iOS app. Select No, if you do not want to assign a license or you do not have a license to assign to the app. 3. If you have assigned a license to the app, in the App license drop-down list, select the VPP account to associate with the app. 4. In the Assign license to drop-down list, assign the license to the User or Device. If no value is specified in the App license drop-down list, the Assign license to drop-down list is not available. 5. Click Assign. <p>Users must follow the instructions to enroll in your organization's VPP on their devices before they can install prepaid apps. Users have to complete this task once.</p> <p>Note: If you grant access to more licenses than you have available, the first users who access the available licenses can install the app. If the app is a required app that does not have an available license, you must obtain the license before the user can install the app or the user will be subject to any compliance rules that you have assigned to the user.</p>

Connect Good Mobile Control to BlackBerry UEM

You can import users from Good Mobile Control to BlackBerry UEM and assign them to a user group in BlackBerry UEM .

Before you begin:

- If you are migrating Microsoft Active Directory users, you must connect BlackBerry UEM to the same Active Directory instance that you are using with Good Mobile Control.
1. In Good Mobile Control, click **Settings > Enterprise Servers**.
 2. Click **Add**.
 3. In the URL field, type the WSDL URL of the BlackBerry UEM console that you want to connect to and enter the log in credentials for the BlackBerry UEM administrator account that you want to use. The WSDL URL is the host name and port number 18084. For example, `https://<hostname>:18084`.
 4. Select the **Enable automatic import of users in BlackBerry UEM** option, if you want to allow users to be automatically added to BlackBerry UEM. When this option is selected, users are imported into BlackBerry UEM when they activate their first BlackBerry Dynamics app.
 5. Select the user group to add the user to in BlackBerry UEM. Make sure that you select a user group that has the BlackBerry Work app assigned to it.

Steps to migrate users

Step	Action
1	In the Good for Enterprise client, turn off Contact Sync.
2	On iOS devices, remove the MDM profile.
3	Instruct users to migrate from Good for Enterprise to BlackBerry Work.
5	In BlackBerry Work, turn on Contact Sync.

Remove the GFE MDM profile on iOS devices

Because iOS devices can only have one MDM profile installed, users with MDM managed iOS devices must remove the GFE MDM Profile. Users must complete the following steps to remove the profile:

1. Tap **Settings > General > Profiles & Device Management**.
2. In the **Mobile Device Management** section, tap **GFE MDM Profile**.
3. Tap **Remove Management**.

Migrate from Good for Enterprise to BlackBerry Work

You can send the following instructions to users that are migrating from Good for Enterprise to BlackBerry Work.

1. Open the BlackBerry Work app.
2. Tap **Set up using Good for Enterprise - Auth Delegate**.
3. On the **Work is requesting setup** screen, click **OK**. Wait while the app is activated.
4. When you are prompted, create a password for BlackBerry Work.
5. Tap **I agree** to accept the license agreement.
6. Enter the login credentials for your email account.
7. Tap **Next**. Wait while the account information is synchronized.
8. When you are prompted, tap the BlackBerry Dynamics Launcher icon.

The BlackBerry Work app synchronizes your email messages.

Decommissioning Good for Enterprise

Good for Enterprise and BlackBerry Work can co-exist on the same device. Depending on your organization's mobile device policies, you can allow a transition period for users to become familiar with BlackBerry Work while they still have access to their email and calendar from Good for Enterprise. You can eventually end the transition period using one of the following approaches.

Hard cutoff: You schedule a concrete cutoff date after which cannot access Good for Enterprise. The hard cutoff date is applied and enforced using the Wipe Container option in Good Mobile Control. Notify your users of the impending change through any standard communication channel that your organization uses. Immediately after the cutoff date, users must use BlackBerry Work to access the functionality previously provided by Good for Enterprise. Another option is to modify the policy for end users to make BlackBerry Work the authentication delegate. When the change goes into effect, users cannot use Good for Enterprise without downloading and provisioning BlackBerry Work. When users download and activate BlackBerry Work, they are prompted to create a new password for the new app, where Good for Enterprise and every other BlackBerry Dynamics app will use BlackBerry Work as the authentication delegate.

Soft cutoff: You let your end users choose when to move to the new platform. You provision them in advance to use BlackBerry Work after you create a compliance policy in Good Mobile Control to wipe Good for Enterprise when that device has not connected to the NOC after a set number of days. User entitlement to Good for Enterprise is then removed from the device. The Good for Enterprise app will still need to be uninstalled by the user.

In both cases—hard cutoff or soft cutoff—you can monitor the adoption of BlackBerry Work and the lack of Good for Enterprise usage in the various reports available in Good Mobile Control. For information on how to create and view reports, see the [Good Mobile Messaging Administrator's Guide](#). You can then proactively remove Good for Enterprise from your users' devices or wait for the migration to happen organically.

For guidance on decommissioning the Good Mobile Messaging server, see the [Good Mobile Messaging Administrator's Guide](#).

Legal notice

©2018 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Android is a trademark of Google Inc. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. MicrosoftLync, and SharePoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

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

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

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

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-

PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

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

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

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

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

Published in Canada