



BlackBerry Enterprise BRIDGE

Administration Guide

1.1

Contents

- What is BlackBerry Enterprise BRIDGE?..... 5**
- Architecture: BlackBerry Enterprise BRIDGE.....6**
- Data flow: Sending documents between BlackBerry Work and Microsoft Intune managed apps using the BlackBerry Enterprise BRIDGE app..... 8**
- Data flow: Sending documents between Microsoft Intune-managed apps and BlackBerry Dynamics apps using the BlackBerry Enterprise BRIDGE app..... 9**
- Steps to manage BlackBerry Enterprise BRIDGE..... 10**
- System requirements..... 11**
- Connecting BlackBerry UEM to Microsoft Azure..... 12**
 - Create a Microsoft Azure account..... 12
 - Synchronize Microsoft Active Directory with Microsoft Azure.....12
 - Create an enterprise endpoint in Azure..... 13
 - Configuring BlackBerry UEM to synchronize with Microsoft Intune..... 14
 - Configure BlackBerry UEM to synchronize with Microsoft Intune in BlackBerry UEM..... 14
- Managing the BlackBerry Enterprise BRIDGE app..... 15**
 - Adding the Intune managed mobile apps to the app list..... 15
 - View public BlackBerry Dynamics app entitlements..... 15
 - Update the app list..... 15
- Creating directory-linked groups..... 16**
 - Create a directory-linked group..... 16
- Managing apps protected by Microsoft Intune..... 18**
 - Create a Microsoft Intune app protection profile in BlackBerry UEM..... 18
 - Turn off interoperability between BlackBerry Dynamics apps and app managed by Intune in BlackBerry UEM..... 19
 - Assign the Intune app protection profile to a directory-linked group in BlackBerry UEM..... 19

- Options for installing and activating BlackBerry Enterprise BRIDGE..... 21**
 - Install BlackBerry Enterprise BRIDGE using the BlackBerry UEM Client on iOS devices..... 21
 - Install BlackBerry Enterprise BRIDGE using the BlackBerry UEM Client on Android devices..... 22
 - Install BlackBerry Enterprise BRIDGE from the App Store on iOS devices..... 23
 - Install BlackBerry Enterprise BRIDGE from Google Play on Android devices..... 24

- Wipe apps managed by Microsoft Intune..... 25**

- Troubleshooting..... 26**
 - Change the log level to Warn for Microsoft Intune customers..... 26
 - Upload log files to BlackBerry Support..... 26
 - Send feedback to BlackBerry..... 26
 - Unable to save a copy of a file in the Intune-managed app..... 27

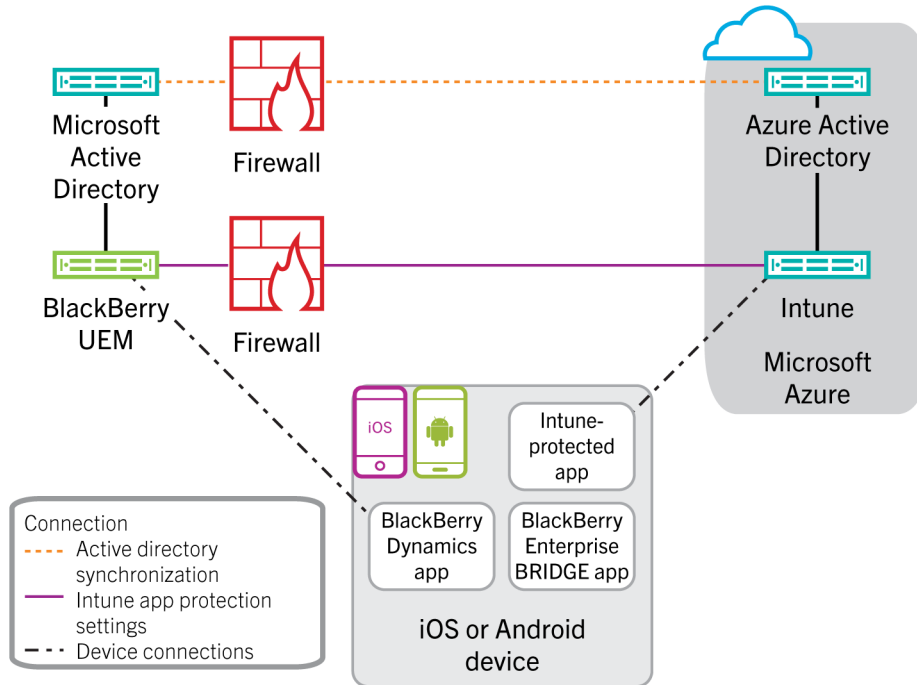
- Legal notice..... 28**

What is BlackBerry Enterprise BRIDGE?

BlackBerry Enterprise BRIDGE is a Microsoft Intune app that is enabled for BlackBerry Dynamics. It allows you to securely view, edit, and save documents using Intune managed Microsoft apps, such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel in BlackBerry Dynamics on iOS and Android devices. The following are the features of BlackBerry Enterprise BRIDGE.

Feature	Description
Secure sharing and storing of data	Share your documents as email attachments (requires BlackBerry Work). Maintain data encryption during the document-sharing process between BlackBerry Dynamics apps and Intune managed mobile apps.
Document access, create, and editing	Access documents while you are on the go from native Microsoft mobile apps. View, create, edit, and save documents.
User experience	Seamlessly transfer files to native Microsoft mobile apps from within BlackBerry Work and from native Microsoft mobile apps to BlackBerry Dynamics apps.
Document fidelity	Documents are rendered with Microsoft native fidelity on all devices.
PDF slide show presentation tool	On iOS devices, use BlackBerry Enterprise BRIDGE to present PDF slide shows.

Architecture: BlackBerry Enterprise BRIDGE



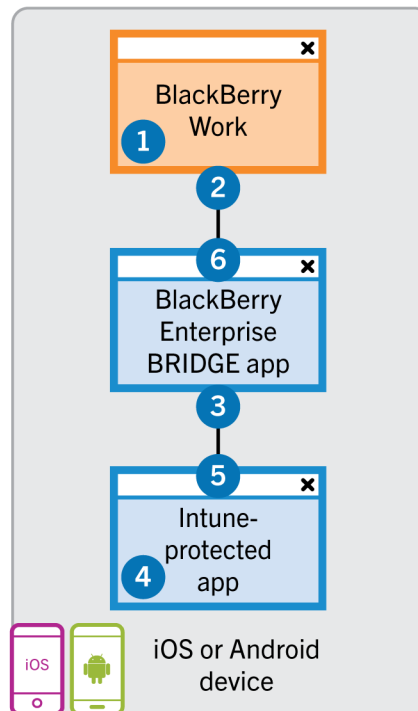
Note: Each directory-linked group can link to only one company directory. For example, if BlackBerry UEM has two Microsoft Active Directory connections (A and B), and you create a directory-linked group that is linked to connection A, you can link only to directory groups from connection A. You must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

Component	Description
BlackBerry UEM Core	The BlackBerry UEM Core is the central component of the BlackBerry UEM architecture. It consists of several subcomponents that are responsible for: <ul style="list-style-type: none"> Logging, monitoring, reporting, and management functions Authentication and authorization services for the BlackBerry UEM Core local directory and company directories Scheduling and sending commands, IT policies, and profiles to devices
Microsoft Intune	Microsoft Intune is a cloud-based EMM service that provides both MDM and MAM features. Intune MAM provides security features for apps such as Microsoft Office 365 that protect data within apps.
Microsoft Azure	Microsoft Azure is the Microsoft cloud computing service for deploying and managing apps and services.

Component	Description
Microsoft Graph API	The Microsoft Graph API connects the BlackBerry UEM MAM and Intune app protection profile to Intune and synchronizes the Microsoft Intune app protection profile settings to Intune. This is one-way synchronization from BlackBerry UEM to Intune.
Devices	The BlackBerry Enterprise BRIDGE app is supported on Android and iOS devices.

Data flow: Sending documents between BlackBerry Work and Microsoft Intune managed apps using the BlackBerry Enterprise BRIDGE app

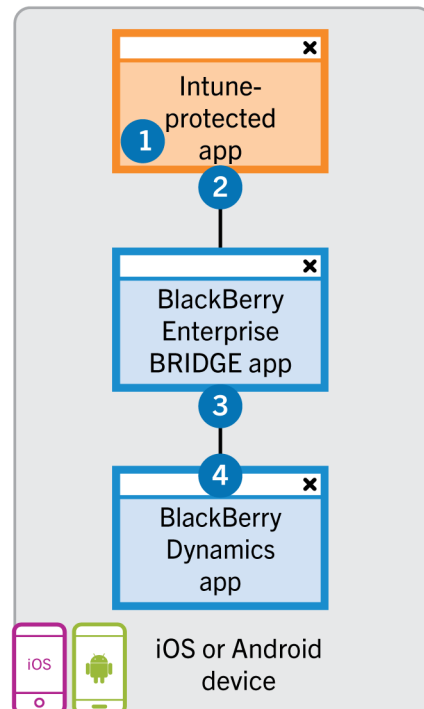
This data flow shows how to share documents that are received as email attachments in BlackBerry Work or saved to the Local Docs folder or an Enterprise remote Docs location to Intune managed apps on Android and iOS devices when the Enterprise BRIDGE app is installed. In this example, a user opens a Microsoft Word document that has been received as an email attachment and that requires feedback.



1. The user downloads and previews a file received as an email attachment in BlackBerry Work.
2. If the Microsoft Intune app protection policy profile allows it, the device sends a copy of the file using the AppKinetics Transfer File service through secured channels to the Enterprise BRIDGE app.
3. The Enterprise BRIDGE app securely sends a copy of the file over an Intune protected channel to the Intune managed app (for example, Microsoft Word). The Enterprise BRIDGE app deletes the copy of the file within the Enterprise BRIDGE app after the file transfer is complete.
4. The user performs the following actions:
 - a. Saves a copy of the file in an Intune protected area of the Intune managed app.
 - b. Modifies the file as required and saves the updated file.
5. The device sends a copy of the file back to the Enterprise BRIDGE app over the Intune protected channel.
6. The Enterprise BRIDGE app sends the copy of the file to BlackBerry Work using the AppKinetics Transfer File service through secured channels to attach to the original or a new email or to save to the Local Docs folder or an Enterprise remote Docs location. The Enterprise BRIDGE app deletes the copy of the file within the Enterprise BRIDGE app after the file transfer is complete.

Data flow: Sending documents between Microsoft Intune-managed apps and BlackBerry Dynamics apps using the BlackBerry Enterprise BRIDGE app

This data flow shows how to share documents that are created in supported Intune-managed apps and BlackBerry Dynamics apps on Android and iOS devices when the Enterprise BRIDGE app is installed. In this example, a user creates a new file in Microsoft Word and sends the file to the manager for review.



1. The user performs the following actions:
 - Creates a file in Microsoft Word.
 - Saves a copy of the file in an Intune protected area of the Intune-managed app.
2. The device sends a copy of the file to the Enterprise BRIDGE app over the Intune protected channel.
3. The user selects to Send Email.
4. If the Microsoft Intune app protection policy profile allows it, the Enterprise BRIDGE app sends a copy of the file to BlackBerry Work using the AppKinetics Transfer File service through secured channels to attach to an email (or to save to the Local Docs folder or an Enterprise remote Docs location). The Enterprise BRIDGE app deletes the copy of the file within the Enterprise BRIDGE app after the file transfer is complete.

Steps to manage BlackBerry Enterprise BRIDGE

When you configure your environment for BlackBerry Enterprise BRIDGE, you perform the following actions.

Note: Some of these tasks might have been completed when you installed and configured BlackBerry UEM.

Step	Action
1	Review system requirements.
2	Install BlackBerry UEM or upgrade to the latest version of BlackBerry UEM. For instructions, see the BlackBerry UEM Installation and Upgrade content.
3	Connect BlackBerry UEM to Microsoft Azure.
4	Configure BlackBerry UEM to synchronize with Microsoft Intune.
5	Configure BlackBerry Work and make it available to users. For instructions, see the BlackBerry Work administration content for details.
6	Make the BlackBerry Enterprise BRIDGE app available to users. Optionally, users can download and install the app from the App Store or Google Play.
7	Make the Microsoft PowerPoint, Microsoft Word, and Microsoft Excel apps available to users. Users can download and install the apps from the App Store or Google Play.
8	Create one or more directory-linked groups and assign the apps to the directory-linked group
9	Assign a Microsoft Intune app protection profile to a directory-linked group.
10	Instruct users to install and activate the BlackBerry Enterprise BRIDGE app on their devices.

System requirements

To use BlackBerry Enterprise BRIDGE, your organization must meet the following requirements:

Item	Description
Server requirements	<ul style="list-style-type: none">• On-premises BlackBerry UEM version 12.8 or later• BlackBerry UEM must be connected to a Microsoft Active Directory instance. For more information, see the BlackBerry UEM Configuration content for details.• Microsoft Intune tenant in Microsoft Azure
Services	Microsoft Azure account with appropriate permissions and required licenses. For more information about account permissions, visit https://support.blackberry.com/kb to read article 50341.
Device OS	<ul style="list-style-type: none">• For device OS compatibility, see the Mobile/Desktop OS and Enterprise Applications Compatibility Matrix
Apps	<ul style="list-style-type: none">• The following apps and required licenses:<ul style="list-style-type: none">• Microsoft Word• Microsoft PowerPoint• Microsoft Excel• One or more BlackBerry Dynamics apps for example, BlackBerry Work version 2.12 or later and entitlement• For Android devices, make sure that the Microsoft Intune Company Portal app is installed on devices but not activated. For more information, see https://docs.microsoft.com/intune/app-protection-enabled-apps-android.

Connecting BlackBerry UEM to Microsoft Azure

Microsoft Azure is the Microsoft cloud computing service for deploying and managing apps and services. You must connect BlackBerry UEM to Azure if you want to use BlackBerry UEM to deploy iOS and Android apps managed by Microsoft Intune.

Note: You must use the Microsoft Azure account with appropriate permissions to complete these tasks. For more information about account permissions, visit <https://support.blackberry.com/kb> to read article 50341.

BlackBerry UEM supports configuring only one Azure tenant. To connect BlackBerry UEM to Azure, you perform the following actions:

Step	Action
1	Create a Microsoft Azure account.
2	Synchronize Microsoft Active Directory with Microsoft Azure.
3	Create an enterprise endpoint in Azure.
4	Configure BlackBerry UEM to synchronize with Microsoft Intune.

Create a Microsoft Azure account

To deploy apps protected by Microsoft Intune to iOS and Android devices in BlackBerry UEM, you must have a Microsoft Azure account and authenticate BlackBerry UEM with Azure.

Complete this task if your organization doesn't have a Microsoft Azure account.

1. Go to <https://azure.microsoft.com> and click **Free account**. Follow the instructions to create the account.
You are required to provide credit card information to create the account.
2. Sign in to the Azure management portal at <https://portal.azure.com> and log in with the username and password you created when you created your account.

After you finish: [Synchronize Microsoft Active Directory with Microsoft Azure.](#)

Synchronize Microsoft Active Directory with Microsoft Azure

To send apps protected by Microsoft Intune to iOS and Android devices, users must exist in the Microsoft Azure directory. Synchronize users and groups between your on-premises Active Directory and Azure Active Directory using Microsoft Azure Active Directory Connect. For more information, visit <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>.

Before you begin: [Create a Microsoft Azure account](#)

1. Download Azure AD Connect from <http://www.microsoft.com/en-us/download/details.aspx?id=47594>.
2. Install the Azure AD Connect software.
3. Configure Azure AD Connect to connect your on-premises Active Directory with the Azure Active Directory.

After you finish: [Create an enterprise endpoint in Azure](#)

Create an enterprise endpoint in Azure

To provide BlackBerry UEM access to Microsoft Azure you must create an enterprise endpoint within Azure. The enterprise endpoint allows BlackBerry UEM to authenticate with Microsoft Azure. For more information, see <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration>.

If you are connecting BlackBerry UEM to both Microsoft Intune and the Windows Store for Business, use a different enterprise application for each purpose to avoid issues with different permissions and potential future changes.

Note: Creating the app to use Microsoft Intune (step 10), must be completed using the Azure account with Global administrator permissions.

Before you begin: [Synchronize Microsoft Active Directory with Microsoft Azure](#)

1. Log in to the [Azure portal](#).
2. Go to **Microsoft Azure > Azure Active Directory > App registrations**.
3. Click **Endpoints**.
4. Copy the **OAUTH 2.0 TOKEN ENDPOINT** value and paste it to a text file.
This is the **OAUTH 2.0 token endpoint** required in BlackBerry UEM.
5. Close the **Endpoints** list and select **New application registration**.
6. Enter the following information for your app:

Field	Setting
Name	<A name for your application>
Application type	Web app or API
Sign-on URL	Any valid URL Note: If you don't have a registered domain you can use: http://localhost/

7. Click **Create**.
8. Click on the app you just created.
9. Copy the **Application ID** of your app and paste it to a text file.
This is the **Client ID** required in BlackBerry UEM.
10. Create the app to use Microsoft Intune, click **Required permissions** in the **Settings** menu. Perform the following steps.
 - a) Click **Add**.
 - b) Click **Select an API**.
 - c) Select **Microsoft Graph**.
 - d) Click **Select**.

- e) Scroll down in the permissions list and under **Delegated Permissions**, set the following permissions for Microsoft Intune:
 - Read and write Microsoft Intune apps (preview)
 - Read all users' basic profile
 - Read all groups
- f) Click **Select**.
- g) Click **Done**.
- h) Click **Grant Permissions** in the **Required permissions** pane.
- i) When prompted, click **Yes** to grant permissions for all accounts in the current directory.

11. Select **Keys** in the **Settings** menu. Perform the following actions:

- a) Enter a name for your key.
- b) Select a duration for your key.
- c) Click **Save**.
- d) Copy the value of your key.

This is the **Client Key** that is required in BlackBerry UEM.



Warning: If you do not copy the value of your key at this time, you will have to create a new key because the value is not displayed after you leave this screen.

After you finish: [Configure BlackBerry UEM to synchronize with Microsoft Intune in BlackBerry UEM.](#)

Configuring BlackBerry UEM to synchronize with Microsoft Intune

Microsoft Intune is a cloud-based EMM service that provides both MDM and MAM features. Intune MAM provides security features for apps, including Office 365 apps, that protect data within apps. For example, Intune can require that data within apps be encrypted and prevent copying and pasting, printing, and using the Save as command.

After you connect BlackBerry UEM to Microsoft Intune, you can use the UEM management console to create and modify Microsoft Intune app protection profiles.

Before you configure BlackBerry UEM to synchronize with Microsoft Intune, you must [connect BlackBerry UEM to Microsoft Azure](#).

Configure BlackBerry UEM to synchronize with Microsoft Intune in BlackBerry UEM

Before you begin: [Create an enterprise endpoint in Azure](#)

1. Log in to the BlackBerry UEM management console.
2. Click **Settings > External Integration > Microsoft Intune**.
3. Enter the information you copied from the Azure portal when you created the enterprise app in Azure.
 - **Client ID:** The app ID generated by the Azure app registration
 - **Client key:** The client secret generated by the Azure app registration
 - **OAuth 2.0 token endpoint:** The tenant specific OAuth endpoint URL for requesting authentication tokens
 - **Username:** The account that BlackBerry UEM uses to access Intune. Visit <https://support.blackberry.com/kb> to read article 50341 for information on the permissions required for the Intune administrator account.
 - **Password:** The password for the Intune administrator account
4. Click **Next**.

After you finish: [Create a Microsoft Intune app protection profile](#)

Managing the BlackBerry Enterprise BRIDGE app

You can manage and monitor the BlackBerry Enterprise BRIDGE app on iOS and Android devices. To manage the app, you can add the public BlackBerry Enterprise BRIDGE app from the [BlackBerry Marketplace for Enterprise Software](#) to the app list in the BlackBerry UEM console and assign it to user accounts or directory-linked groups.

To permit users to use BlackBerry Enterprise BRIDGE, you must purchase the entitlement (com.blackberry.intune.bridge) and assign it to each user that you assign the BlackBerry Enterprise BRIDGE app to.

Adding the Intune managed mobile apps to the app list


You can add the Microsoft Intune managed mobile apps, Microsoft Word, Microsoft PowerPoint, and Microsoft Excel to the app list from the App Store or Google Play. After the apps are added to the app list, you can assign them to users. Optionally, users can download the apps from the App Store or Google Play. For more information about adding [iOS apps](#) or [Android apps](#) to the app list, see the BlackBerry UEM administration content.

View public BlackBerry Dynamics app entitlements

1. Log in to <https://account.good.com/pce/#/a/organization//servers>.
2. Expand **Entitlements**.

Update the app list

You can update the app list to make sure that you have the latest information about iOS and Android apps in the apps list. Updating the app information does not mean that the app is updated on a user's device. Users receive update notifications for their work apps in the same way that they receive update notifications for their personal apps.

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

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.

Important: You must create directory-linked groups because Microsoft Intune app protection profiles can be assigned only to directory-linked groups. The directory-linked group must be a security group in Microsoft Active Directory. If the group is a distribution group, users won't have the appropriate permissions and cannot log in after the BRIDGE app is installed on their device. For more information on Microsoft Intune app protection profiles, see [Managing apps protected by Microsoft Intune](#)

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](#).

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](#).

Create a directory-linked group

Before you begin:

- Enable directory-linked groups. For instructions, [see the Configuration content](#).
- Make sure that the directory-linked group is a security group and not a distribution group in Microsoft Active Directory.

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**.

Managing apps protected by Microsoft Intune

For iOS and Android devices, if you want to use Microsoft Intune app protection policies to protect data in Office 365 apps, you can do so while using BlackBerry UEM to manage the devices. You can connect UEM to Intune, allowing you to set Intune app protection policies from within the UEM management console.

To deploy apps protected by Intune, you must first configure the connection between UEM and Intune. For more information, see [Connecting BlackBerry UEM to Microsoft Azure](#).

Intune uses app protection policies to protect apps. To protect apps from the UEM management console, you create an Intune app protection profile. When you create or update an app protection profile in UEM, the settings are sent to Intune and update the settings in the corresponding app protection policy.



Warning:

- If you update the Intune app protection policy in the Azure portal, the changes are not synchronized with BlackBerry UEM. After you create an app protection profile in UEM, do not update the corresponding Intune policy within Azure. Modifying or deleting the Intune policy can prevent other users from activating BlackBerry Enterprise BRIDGE.
- Creating an Intune policy in Azure and assign it to a directory-linked group that includes users that are managed by BlackBerry UEM is not supported.

Create a Microsoft Intune app protection profile in BlackBerry UEM

When you create or update a Microsoft Intune app protection profile in BlackBerry UEM, the profile settings are sent to Intune to update the corresponding app protection policy. Microsoft Intune app protection profiles can be assigned only to directory-linked groups.




Warning: The Microsoft Intune app protection profile settings are sent to Intune and update the settings in the corresponding app protection policy. Modifying or deleting the Intune policy in Azure can prevent other users from activating BlackBerry Enterprise BRIDGE.

For more information about Microsoft Intune app protection profile settings, see [Microsoft Intune app protection profile settings in the BlackBerry UEM administration content](#). If you configure the Microsoft Intune app protection profile to Prevent Save as and allow users to save files to a Local storage, users receive the error message "Action Not Allowed. Your organization only allows you to open work or school data in this app" when they try to send a file from the device not secure local storage. Files must be opened from a corporate location (for example, a secured local storage, Microsoft OneDrive for Business or Microsoft SharePoint).

Before you begin:

- [Configure BlackBerry UEM to synchronize with Microsoft Intune](#). The Microsoft Intune app protection profile does not appear on the Policies and Profiles page if the connection isn't configured.
 - For Android devices, make sure the Microsoft Company Portal app is installed on devices but not activated. For more information, see <https://docs.microsoft.com/intune/app-protection-enabled-apps-android>.
1. On the menu bar, click **Policies and Profiles**.
 2. Click **Protection > Microsoft Intune app protection profile**.
 3. Click **+**.
 4. Type a name and description for the profile.
 5. Select the **Enable interoperability between Intune and Dynamics apps** checkbox.

When you enable this feature, the following policy settings are set to Policy Managed apps only and cannot be changed for security reasons such as enforcing data to remain within the Intune protected secure environment:


- Allow app to transfer data to other apps
 - Allow app to receive data from other apps
6. Optionally, in the custom JSON field, edit the JSON values if you want to customize messages and warning seen by your users in the Enterprise BRIDGE app.
 7. Select the **Prevent Save as** checkbox and select one or more of the following options to allow users to save files to the following locations:
 - Local storage: Allows users to save a copy of the file in the Intune-managed app.
 - OneDrive for Business
 - SharePoint
 8. Beside the App package IDs, click .
 9. Select the following apps:
 - com.microsoft.office.excel
 - com.microsoft.office.powerpoint
 - com.microsoft.office.word
 10. Click **Save**.
 11. Click **Add**.

After you finish: [Assign the Intune app protection profile to a directory-linked group.](#)

Turn off interoperability between BlackBerry Dynamics apps and app managed by Intune in BlackBerry UEM

You can turn off interoperability between the BlackBerry Enterprise BRIDGE app and Intune managed apps. Turning off interoperability causes the BlackBerry Enterprise BRIDGE app to stop working, but does not affect the functionality of other Intune managed apps. For example, users can view the content of a Microsoft Word file, but the files are not opened in the Intune protected area of Microsoft Word. The BlackBerry Enterprise BRIDGE app is not uninstalled from the device.

Before you begin: [Create a Microsoft Intune app protection profile.](#)

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Microsoft Intune app protection** profile.
3. Click the Microsoft Intune app protection profile that you want to turn off the interoperability feature for.
4. Click .
5. Clear the **Enable interoperability between Intune and Dynamics apps** checkbox.
6. Click **Save**.

Assign the Intune app protection profile to a directory-linked group in BlackBerry UEM

Before you begin: [Create a Microsoft Intune app protection profile in BlackBerry UEM.](#)



Warning: If users are members of multiple directory-linked groups and each group is assigned a different Microsoft Intune app protection profile, the BlackBerry Enterprise BRIDGE app might not activate successfully or function as expected.

1. On the menu bar, click **Groups**.
2. Search for the directory-linked group.
3. In the search results, click the name of the directory-linked group.
4. On the **Settings** tab, in the **Assigned profile** section, click **+**.
5. Click **Microsoft Intune app protection profile**.
6. In the drop-down list, click the name of the Intune app protection profile that you want to assign to the group.
7. Click **Assign**.

Options for installing and activating BlackBerry Enterprise BRIDGE

Before users can begin using BlackBerry Enterprise BRIDGE, it must be activated. The steps that users take to install the app depends on how you have configured your environment. If you have not yet configured your activation settings, [see the BlackBerry UEM administration content](#) for steps on how to configure your environment to support BlackBerry Dynamics apps.

The following options are available for activating BlackBerry Enterprise BRIDGE on iOS and Android devices:

- Install and activate BlackBerry Enterprise BRIDGE using the BlackBerry UEM Client: This option provides users with a consistent, streamlined activation experience. Users need only their email address and an activation password and do not require an access key. Users must install the UEM Client to activate their devices with MDM. For this option to be available to users, you must [allow the UEM Client to manage the activation of BlackBerry Dynamics apps](#).
- Install and activate BlackBerry Enterprise BRIDGE from the App Store or Google Play: Users choose this option if they are downloading and installing on their device, if they have not installed the UEM Client, or if you have not allowed the BlackBerry UEM Client to manage the activation of BlackBerry Dynamics apps.

Install BlackBerry Enterprise BRIDGE using the BlackBerry UEM Client on iOS devices

You can send the following instructions to iOS and Android device users that are installing BlackBerry Enterprise BRIDGE using the BlackBerry UEM Client.

Before you begin:

- Make sure that a BlackBerry Dynamics app, for example, BlackBerry Work, is installed and activated on your device.
 - Make sure that the supported Microsoft Intune-managed apps are installed and activated on your device.
1. If the app was not automatically pushed to your device by your administrator, open your Work Apps app and install the BlackBerry Enterprise BRIDGE app. If you do not see the BlackBerry Enterprise BRIDGE app in your Work Apps app, contact your administrator to make the app available to you.
 2. On your device, tap **BB Bridge**.
 3. Tap **Login**.
 4. On the **Microsoft Sign in** page, enter your email address.

Note: You must log in to the BlackBerry Enterprise BRIDGE app using the same email address that you use for BlackBerry Work. Using a different email address to log in is not supported.

5. Tap **Next**.
6. If your organization has a login page, enter your username.
7. Tap **Next**.
8. Enter your password.
9. Tap **Sign in**.
10. Tap **OK** to acknowledge that your organization protects the data in the app and to restart the app.
11. Tap **BB Bridge**.
12. If prompted, set a PIN or use Touch ID to access your organization's data using the BlackBerry Enterprise BRIDGE app.

13. Read the license agreement and if you agree, tap **I agree**.
14. To activate the BlackBerry Enterprise BRIDGE app, enter your password for the BlackBerry Dynamics app that is displayed in the activation request. For example, BlackBerry Work or BlackBerry UEM Client.
15. Tap **OK**.
16. If this is the first time that you have logged in to the BlackBerry Enterprise BRIDGE app, the Tutorials screen opens and displays a list of two tutorials. You can view one or both of the tutorials or tap **Close** to close the Tutorials screen.
17. In the reminder dialog box, tap **OK**. You can view the tutorial later from the Settings screen.

Install BlackBerry Enterprise BRIDGE using the BlackBerry UEM Client on Android devices

You can send the following instructions to Android device users that are installing BlackBerry Enterprise BRIDGE using the BlackBerry UEM Client.

Before you begin:

- Make sure the Microsoft Intune Company Portal app is installed on your device. You do not need to activate the app. For more information, see <https://docs.microsoft.com/intune/app-protection-enabled-apps-android>.
 - Make sure that the supported Microsoft Intune managed apps are installed and activated on your device.
 - Make sure that a BlackBerry Dynamics app, for example, BlackBerry Work, is installed and activated on your device.
1. If the app was not automatically pushed to your device by your administrator, open your Work Apps app and install the BlackBerry Enterprise BRIDGE app. If you do not see the BlackBerry Enterprise BRIDGE app in your Work Apps app, contact your administrator to make the app available to you.
 2. On your device, tap **BRIDGE**.
 3. Tap **Login**
 4. If the Intune Company Portal app is not installed on your device, you are prompted with the **To use your work or school account with this app, you must install the Intune Company Portal app. Tap "Play Store" to continue** message. Tap **Play Store** to install the Microsoft Intune Company Portal app.
 5. Tap **Login**
 6. On the **Microsoft Sign in** page, enter your email address.
Note: You must log in to the BlackBerry Enterprise BRIDGE app using the same email address that you use for BlackBerry Work. Using a different email address to log in is not supported.
 7. Tap **Next**.
 8. On your organization's login page, enter your username.
 9. Tap **Next**.
 10. Enter your password.
 11. Tap **Sign in**.
 12. Click **OK**, to acknowledge that your IT department is helping to protect your work or school data using the Enterprise BRIDGE app.
 13. To activate the BlackBerry Enterprise BRIDGE app, enter your password for the BlackBerry Dynamics app that is displayed in the activation request. For example, BlackBerry Work or BlackBerry UEM Client.
 14. Click **OK**, to acknowledge that your organization protects the data in the app and to restart the app.
 15. If BlackBerry Work opens, place it in the background.

- 16.If you are prompted, set a PIN or use your fingerprint to access your organization's data using the BlackBerry Enterprise BRIDGE app.
- 17.Confirm the PIN.
- 18.Read the license agreement and if you agree, tap **Accept**.
- 19.If this is the first time that you have logged in to the Enterprise BRIDGE app, the tutorial opens. Complete one of the following tasks:
 - Tap **Skip** to close the tutorial. Tap **OK**. You can view the tutorial later from the Settings screen.
 - View the Tutorial. Click **Done**. A reminder prompt is not displayed, but the tutorial is available in the Settings screen to view again.

Install BlackBerry Enterprise BRIDGE from the App Store on iOS devices

You can send the following instructions to iOS device users that are installing the BlackBerry Enterprise BRIDGE app on devices that don't have the BlackBerry UEM Client installed, or if you didn't allow the UEM Client to manage the activation of the BlackBerry Enterprise BRIDGE app.

Before you begin:

- Make sure that a BlackBerry Dynamics app, for example, BlackBerry Work, is installed and activated on your device. For instructions, see the [BlackBerry Work user guide for your device](#).
 - Make sure that the supported Microsoft Intune managed apps are installed and activated on your device.
1. Download the BlackBerry Enterprise BRIDGE app from the App Store.
 2. Tap **BB Bridge**.
 3. Tap **Login**.
 4. On the **Microsoft Sign in** page, enter your email address field.

Note: You must log in to the BlackBerry Enterprise BRIDGE app using the same email address that you use for BlackBerry Work. Using a different email address to log in is not supported.
 5. Tap **Next**.
 6. If your organization has a login page, enter your username.
 7. Tap **Next**.
 8. Enter your password.
 9. Tap **Sign in**.
 - 10.Tap **OK** to acknowledge that your organization protects the data in the app and to restart the app.
 - 11.Tap **BB Bridge**.
 - 12.If prompted, set a PIN to access your organizations data using the BlackBerry Enterprise BRIDGE app.
 - 13.Read the license agreement and if you agree, tap **I agree**.
 - 14.To activate the BlackBerry Enterprise BRIDGE app, enter your password for the BlackBerry Dynamics app or use Touch ID.
 - 15.Tap **OK**.
 - 16.If this is the first time you have logged in to the BlackBerry Enterprise BRIDGE app, the Tutorials screen opens and displays a list of two tutorials. You can view one or both of the tutorials or tap **Close** to close the Tutorials screen
 - 17.Click **OK**. You can view the tutorial later from the Settings screen.

Install BlackBerry Enterprise BRIDGE from Google Play on Android devices

You can send the following instructions to device users that are installing the BlackBerry Enterprise BRIDGE app on their devices.

Before you begin:

- Make sure that a BlackBerry Dynamics app, for example, BlackBerry Work, is installed and activated on your device.
- Make sure the Microsoft Intune Company Portal app is installed on your device. You do not need to activate the app. For more information, see <https://docs.microsoft.com/intune/app-protection-enabled-apps-android>.
- Make sure that the supported Microsoft Intune managed apps are installed and activated on your device.

1. Download the BlackBerry Enterprise BRIDGE app from Google Play.
2. Tap **BRIDGE**.
3. Tap **Login**.
4. Tap **Login**.
5. On the **Microsoft Sign in** page, enter your email address.
Note: You must log in to the BlackBerry Enterprise BRIDGE app using the same email address that you use for BlackBerry Work. Using a different email address to log in is not supported.
6. Tap **Next**.
7. If your organization has a login page, enter your username.
8. Tap **Next**.
9. Enter your password.
10. Tap **Sign in**.
11. Click **OK** to acknowledge that your IT department is helping to protect your work or school data using the Enterprise BRIDGE app.
12. To activate the BlackBerry Enterprise BRIDGE app, enter your password for the BlackBerry Dynamics app or use your fingerprint.
13. Click **OK** to acknowledge that your organization protects the data in the app and to restart the app.
14. If BlackBerry Work opens, place it in the background.
15. If you are prompted, set a PIN or use your fingerprint to access your organization's data using the BlackBerry Enterprise BRIDGE app.
16. Confirm the PIN.
17. Read the license agreement and if you agree, tap **Accept**.
18. If this is the first time you have logged in to the BlackBerry Enterprise BRIDGE app, the tutorial opens. Complete one of the following tasks:
 - Tap **Skip** to close the tutorial. Tap **OK**. You can view the tutorial later from the Settings screen.
 - View the Tutorial. Click **Done**. A reminder prompt is not displayed, but the tutorial is available in the Settings screen to view again.

Wipe apps managed by Microsoft Intune

You can use the Wipe apps command to delete the data from apps that are managed by Intune on iOS and Android devices. The apps are not uninstalled when this command is sent.

1. On the menu bar, click **Users**.
2. Search for and click the user that you want to wipe the data from.
3. Click the *<device model>* (**Intune**) tab.
4. Click **Wipe apps**.

Troubleshooting


Change the log level to Warn for Microsoft Intune customers

If you use Microsoft Intune, you should change the log level to Warn.

1. On the BlackBerry UEM server that you want to change the log level for, locate the log4J.xml file. The default location of the file is `C:\Program Files\BlackBerry\BES\Core\tomcat-core\webapps\ROOT\WEB-INF\classes`
2. In the file, above the `<root>` value, add the following information: `<logger name="org.apache.http.wire"> <level value="warn"/> </logger>`
3. Restart the BlackBerry UEM Core service.

Upload log files to BlackBerry Support


If BlackBerry Support requests log files, you can instruct users to upload log files to help troubleshoot issues that the users are having with the BlackBerry Enterprise BRIDGE app. Depending on the size of the logs, instruct users to allow a short period before they close the Settings screen or place the app in the background to allow the logs to be uploaded to BlackBerry.

1. Open the BlackBerry Enterprise BRIDGE app.
2. Tap .
3. Tap **Send Logs to BlackBerry**.
4. Tap **OK**.

Send feedback to BlackBerry

Users can submit feedback to BlackBerry about the BlackBerry Enterprise BRIDGE app.

Note: This option requires a BlackBerry Dynamics app that supports email to be installed and activated on the device (for example, BlackBerry Work). If users uninstall BlackBerry Work and try to submit feedback, the following error message is displayed: Error - Your device doesn't have a secure email app installed.

1. Open the Enterprise BRIDGE app.
2. Tap .
3. Tap one of the following:
 - On iOS devices, tap **Feedback**.
 - On Android devices, **Send feedback**.
4. On the **Comments** page, type your feedback. By default, the option to send logs to BlackBerry is enabled.
5. Tap **Send**.
6. BlackBerry Work opens and an email message with the proper recipient name, subject line, app details, and feedback is prepopulated for you. Tap the **Send** icon.


Unable to save a copy of a file in the Intune-managed app

Possible cause

Microsoft Intune app protection profile is configured to prevent saving files in a local storage.

Possible solution

Verify users can save files to the local storage.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Microsoft Intune app protection profile**.
3. Click the profile that you want to change.
4. Click .
5. In the **Data relocation** section, select the **Prevent Save as** check box.
6. Select the **Local storage** check box.
7. Click **Save**.

Legal notice

©2019 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 United States and certain other countries. Microsoft, Azure, Excel, Microsoft Intune, and PowerPoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Touch ID is a trademark of Apple Inc. 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, MERCHANTABILITY, 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