



BlackBerry UEM

Managing apps

Administration

12.11

Contents

Apps.....	6
Adding apps to the app list.....	7
Adding public apps to the app list.....	7
Add an iOS app to the app list.....	7
Add an Android app to the app list if BlackBerry UEM is configured for Android Enterprise devices....	9
Add an Android app to the app list if BlackBerry UEM is not configured for Android Enterprise devices.....	10
Add a Windows 10 app to the app list.....	11
Add a BlackBerry 10 app to the app list.....	14
Adding internal apps to the app list.....	15
Steps to add internal apps to the app list.....	15
Specify the shared network location for storing internal apps.....	15
Add an internal app to the app list.....	16
Host an internal app for Android Enterprise devices in Google Play using the .apk file.....	17
Host an internal app for Android Enterprise devices in BlackBerry UEM using a .json file	17
Update an internal app.....	18
Adding app shortcuts.....	18
Create an app shortcut.....	18
Adding or changing an app configuration.....	19
Preventing users from installing specific apps.....	20
Steps to prevent users from installing specific apps.....	20
Add an app to the restricted app list.....	21
Managing apps on the app list.....	22
Delete an app from the app list.....	22
Change whether an app is required or optional.....	22
Device notifications for new and updated apps.....	23
App behavior on iOS devices.....	23
App behavior on Android devices.....	27
App behavior on Android Enterprise devices.....	29
App behavior on Samsung KNOX devices.....	30
App behavior on Windows 10 devices.....	35
App behavior on BlackBerry devices.....	36
Managing app groups.....	37
Create an app group.....	37
Edit an app group.....	38
View the status of apps and app groups assigned to user accounts.....	38
View which apps are assigned to user groups.....	39
Viewing and customizing the apps list.....	39
Select the information to display in the apps list.....	39
Filter the app list.....	39

Update the app list.....	39
Update app permissions for Android Enterprise apps.....	40
Accept app permissions for Android Enterprise apps.....	41
Managing apps protected by Microsoft Intune.....	42
Configuring BlackBerry UEM to synchronize with Microsoft Intune.....	42
Configure BlackBerry UEM to synchronize with Microsoft Intune.....	42
Create a Microsoft Intune app protection profile.....	43
Microsoft Intune app protection profile settings.....	43
Common: Microsoft Intune app protection profile settings.....	43
iOS: Microsoft Intune app protection profile settings.....	46
Android: Microsoft Intune app protection profile settings.....	47
Wipe apps managed by Microsoft Intune.....	48
Managing Apple VPP accounts.....	49
Add an Apple VPP account.....	49
Edit an Apple VPP account.....	49
Update Apple VPP account information.....	50
Delete an Apple VPP account.....	50
Assigning Apple VPP licenses to devices.....	50
View Apple VPP license assignment.....	50
Limiting devices to a single app.....	52
Create an app lock mode profile.....	52
Viewing personal app lists.....	54
View the personal apps list in the management console.....	54
Turn off personal apps collection.....	54
Rating and reviewing apps.....	56
Enable or disable app ratings and reviews for all apps.....	56
Enable app ratings and reviews for existing apps.....	56
View app reviews in the management console.....	57
Specify app rating and review settings for multiple apps.....	57
Delete app ratings and reviews.....	58
Configure the layout of apps on iOS devices.....	59
Managing notifications for apps on iOS devices.....	60
Create a per-app notification profile.....	60
Managing the Work Apps icon for iOS devices.....	62
Customize the Work Apps icon.....	62
Disable the Work Apps app for iOS.....	62

Set the organization name for BlackBerry World.....	63
--	-----------

Managing apps on BlackBerry OS devices.....	64
--	-----------

Preparing to distribute BlackBerry Java Applications	64
Add a BlackBerry Java Application to the shared network folder.....	64
Specify keywords for a BlackBerry Java Application.....	65
Configuring application control policies.....	65
Standard application control policies.....	65
Change a standard application control policy.....	66
Create custom application control policies for a BlackBerry Java Application.....	66
IT policy rules ranking on BlackBerry OS devices.....	67
Application control policies for unlisted applications.....	67
Change the standard application control policy for unlisted applications that are optional.....	68
Create an application control policy for unlisted applications.....	68
Configure the priority of application control policies for unlisted applications.....	68
Creating software configurations.....	69
Steps to create and assign a software configuration.....	69
Create a software configuration.....	69
Add a BlackBerry Java Application to a software configuration.....	70
Install BlackBerry Java Applications on a BlackBerry OS device at a central computer.....	70
View the users that have a BlackBerry Java Application installed on their BlackBerry OS devices.....	71
Reconciliation rules for conflicting settings in software configurations.....	71
Reconciliation rules: BlackBerry Java Applications.....	72
Reconciliation rules: BlackBerry Device Software.....	74
Reconciliation rules: Standard application settings.....	75
Reconciliation rules: Application control policies.....	76
Reconciliation rules: Application control policies for unlisted applications.....	77

Legal notice.....	78
--------------------------	-----------


Apps

You can create a library of apps that you want to manage and monitor on BlackBerry 10, iOS, Android, and Windows devices. To manage apps, you can add the apps to the app list and assign them to user accounts, user groups, or device groups.

When you manage apps, you perform the following actions:

Step	Action
1	Add the public and internal apps that you want to manage to the app list.
2	Create app groups to manage multiple apps at the same time.
3	Assign apps or app groups to user accounts , user groups , or device groups so that users can install them.

Adding apps to the app list

The app list contains apps that you can assign to users, user groups, and device groups. Apps listed with a lock icon  are BlackBerry Dynamics apps.

Note: If your organization uses Microsoft Intune for MAM of apps such as Office 365 apps, instead of adding the apps to the app list, [create a Microsoft Intune app protection profile](#) to assign apps protected by Intune to users.


Adding public apps to the app list

A public app is an app that is available from the BlackBerry World storefront, the App Store online store, the Google Play store, or the Windows Store.

For more information on BlackBerry Dynamics apps, see [Add public BlackBerry Dynamics apps to the app list](#).

Add an iOS app to the app list

When you add public iOS apps to the app list, the connection to the App Store is made directly from the computer that is running the BlackBerry UEM console. If your organization is using a proxy server, you must ensure that no SSL interception occurs. For more information on ports that must be open, [visit support.blackberry.com/community](http://support.blackberry.com/community) to read article 52777.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **App Store**.
4. In the search field, search for the app that you want to add. You can search by app name, vendor, or App Store URL.
5. In the drop-down list, select the country of the store that you want to search in.
6. Click **Search**.
7. In the search results, click **Add** to add an app.
8. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Task	Steps
Select a category for the app	<ol style="list-style-type: none">a. In the drop-down list, select a category.
Create a category for the app	<ol style="list-style-type: none">a. Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside itb. Press Enter.c. Press Enter.

9. In the **App rating and review** drop-down list, perform one of the following actions. When multiple versions of the app exist, the setting specified applies to all versions of the app.
 - If you want users to rate and provide reviews of apps and see all reviews submitted by other users in your environment, select **Public mode**.
 - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.

- If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.

10.In the **Supported device form factor** drop-down list, select the form factors that the app can be installed on. For example, you can prevent the app from being available in the Work Apps app for iPad.

11.If you want the app to be deleted from the device when the device is removed from BlackBerry UEM, select **Remove the app from the device when the device is removed from BlackBerry UEM**. This option applies only to apps with a disposition marked as required and the default installation for required apps is set to prompt once.

12.If you want to prevent apps on iOS devices from being backed up to the iCloud online service, select **Disable iCloud backup for the app**. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.

13.In the **Default installation for required apps** drop-down list, perform one of the following actions:

- If you want users to receive one prompt to install the app on their iOS devices, select **Prompt once**. If users dismiss the prompt, they can install the app later using the Work Apps screen in the BlackBerry UEM Client app or the Work Apps icon on the device.
- If you don't want users to receive a prompt, select **No prompt**.

The default installation method applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.

14.In the **Convert installed personal app to work app** drop-down list, select one of the following:

- To convert the app to a work app if it is already installed, select **Convert**. After you assign the app to a user, the app is converted to a work app and can be managed by BlackBerry UEM.
- If you don't want to convert the app to a work app if it is already installed, select **Do not convert**. After you assign the app to a user, the app cannot be managed by BlackBerry UEM.

15.If the app settings can be preconfigured (for example, connection information), and you want to do so, obtain the configuration details from the app vendor and perform the following actions:

a) In the **App configuration** table, complete one of the following tasks:

Task	Steps
Create an app configuration from an XML template	<ol style="list-style-type: none"> 1. Click + > Create from a template. 2. Click Browse and select the template that you want to add. 3. Click Upload. 4. For each setting, enter the value that you want to set. <p>For more information about app configuration .xml templates, visit http://www.appconfig.org/ios/.</p>
Copy another app configuration	<ol style="list-style-type: none"> 1. Click + > Copy from an app configuration. 2. In the Copy from drop-down list, select the app configuration that you want to copy. 3. For each setting, edit the key name or value.
Create an app configuration manually	<ol style="list-style-type: none"> 1. Click + > Configure manually. 2. For each setting that you want to add, click + and select a value type for the setting. 3. For each setting, enter the key name and the value that you want to set.

b) Type a name in the **App configuration name** field.

- c) Click **Save**.
- d) If necessary, use the arrows to move the profiles up or down the ranking. When an app is assigned more than once with different app configurations, the app configuration with the higher rank applies.

16. Click **Add**.


Add an Android app to the app list if BlackBerry UEM is configured for Android Enterprise devices

If you have configured support for Android Enterprise devices, the connection to Google allows BlackBerry UEM to get app information from Google Play. The connection to Google Play is made directly from the computer that is running the BlackBerry UEM console. If your organization is using a proxy server, you must ensure that no SSL interception occurs. For more information on ports that must be open, [visit support.blackberry.com/community](https://support.blackberry.com/community) to read article 52777. For more information about configuring BlackBerry UEM to support Android Enterprise devices, [see the Configuration content](#)

If BlackBerry UEM is not configured to support Android Enterprise devices, see [Add an Android app to the app list if BlackBerry UEM is not configured for Android Enterprise devices](#).


To use Google Play to manage apps in the Samsung KNOX Workspace, devices must have Samsung KNOX 2.7.1 or later installed and you must allow Google Play app management for Samsung KNOX Workspace devices in the activation profile.

Note: In an upcoming release of BlackBerry UEM, the settings applicable to BlackBerry Hub+ and Divide Productivity will be removed from the email profile and will be available only in an app configuration in the app settings. In this release, if you configure app settings in the email profile and in an app configuration, the app configuration takes precedence if both are assigned.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. Search for the app that you want to add or pick an app on the store home page.
5. Select the app.
6. Click **Approve**.
7. To accept app permissions on behalf of users, click **Approve**. You must accept the app permissions to allow required apps to be automatically installed on Android Enterprise devices or in KNOX Workspace. If you don't accept the app permissions on behalf of users, the app can't be managed in BlackBerry UEM.
8. On the **Approval Settings** tab, choose how you would like to handle new app permission requests when there is an updated app.
 - To automatically accept the new permissions added by the app vendor, select **Keep approved when app requests new permissions**.
 - To manually re-accept the new app permissions added by the app vendor before the app can be sent to new devices, select **Revoke app approval when this app requests new permissions**. For more information about updating app permissions, see [Update app permissions for Android Enterprise apps](#).
9. If you selected the **Revoke app approval when this app requests new permissions** option on the Notifications tab, add a subscriber to be notified when the app permission changes. The administrator will have to re-approve the app before users can access it.
10. Click **Save**.
11. In the **App description** field, type a description for the app.
12. To add screen shots of the app, click **Add** and browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
13. In the **Send to** drop-down list, perform one of the following actions:
 - If you want the app to be sent to all Android devices, select **All Android devices**.

- If you want the app to be sent to only Android devices that use Samsung KNOX Workspace, select **Samsung KNOX Workspace devices**.
- If you want the app to be sent only to Android Enterprise devices, select **Android devices with a work profile**.

14. For apps that support configuration settings, an **App configuration** table is displayed. If you want to create an app configuration, complete the following steps:

- Click  to add an app configuration.
- Type a name for the app configuration and specify the configuration settings to use.
- Click **Save**.
- If necessary, use the arrows to move the profiles up or down the ranking. When an app is assigned more than once with different app configurations, the app configuration with the higher rank applies.

15. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Task	Steps
Select a category for the app	a. In the drop-down list, select a category.
Create a category for the app	a. Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside it b. Press Enter . c. Press Enter .

16. In the **App rating and review** drop-down list, perform one of the following actions. When multiple versions of the app exist, the setting specified applies to all versions of the app.


- If you want users to rate and provide reviews of apps and see all reviews submitted by other users in your environment, select **Public mode**.
- If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
- If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.

17. Click **Add**.

Add an Android app to the app list if BlackBerry UEM is not configured for Android Enterprise devices

Add only apps to the available app list. Movies, music, and newsstand media cannot be delivered to devices. If you assign media to a user and set the disposition of the media as required, the device is subject to the enforcement action defined in the compliance profile that is assigned to it.

If BlackBerry UEM is configured to support Android Enterprise devices, see [Add an Android app to the app list if BlackBerry UEM is configured for Android Enterprise devices](#).

- On the menu bar, click **Apps**.
- Click .
- Click **Google Play**.
- Click **Open Google Play** and search for the app that you want to add. You can then copy and paste information from Google Play in the following steps and also download icons and screen shots.
- In the **App name** field, type the app name.
- In the **App description** field, type a description for the app.

7. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Task	Steps
Select a category for the app	a. In the drop-down list, select a category.
Create a category for the app	a. Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside it b. Press Enter . c. Press Enter .

8. In the **App rating and review** drop-down list, perform one of the following actions. When multiple versions of the app exist, the setting specified applies to all versions of the app.
- If you want users to rate and provide reviews of apps and see all reviews submitted by other users in your environment, select **Public mode**.
 - If you want users to rate and provide reviews of apps only, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
 - If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.
9. In the **Vendor** field, type the name of the app vendor.
10. In the **App icon** field, click **Browse**. Locate and select an icon for the app. The supported formats are .png, .jpg, .jpeg, or .gif. Do not use Google Chrome to download the icon because an incompatible .webp image is downloaded.
11. In the **App web address from Google Play** field, type the web address of the app in Google Play.
12. To add screen shots of the app, click **Add** and browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
13. In the **Send to** drop-down list, perform one of the following actions:
- If you want the app to be sent to all Android devices, select **All Android devices**.
 - If you want the app to be sent to only Android devices that use Samsung KNOX Workspace, select **Only KNOX Workspace devices**.
14. Click **Add**.

Add a Windows 10 app to the app list


To add Windows 10 apps to the app list, you must manage your app catalog in the Windows Store for Business and then synchronize the apps to BlackBerry UEM. When new apps are added to your app catalog, you can synchronize the apps with BlackBerry UEM right away or wait until BlackBerry UEM synchronizes automatically. BlackBerry UEM synchronizes the app catalog every 24 hours.

You can allow users to install offline or online apps from the Windows Store for Business app catalog. Offline apps are downloaded by BlackBerry UEM when you synchronize with the app catalog. Using offline apps is recommended because all management of these apps can be performed from BlackBerry UEM, and users can install them without connecting to the Windows Store for Business. After the apps are installed, devices receive updates to the apps from the Windows Store.

Online apps are downloaded directly from the Windows Store for Business. To be able to send required online apps to devices, instruct your users to add their work accounts to **Accounts used by other apps** in Windows 10.

Before you begin:

- [Specify the shared network location for storing internal apps](#) to store offline apps.
- [Configure BlackBerry UEM to synchronize with the Windows Store for Business](#)

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Windows Store > 10**.
4. Click **Synchronize apps**.

Configuring BlackBerry UEM to synchronize with the Windows Store for Business

If you want to manage Windows 10 apps, you must configure BlackBerry UEM to synchronize with the Windows Store for Business before you can add Windows 10 apps to the app list.

If you later remove the connection to the Windows Store for Business, all of the Windows 10 apps that have been synchronized to BlackBerry UEM will be removed and the apps will be unassigned from users and groups.

When you configure BlackBerry UEM to synchronize with the Windows Store for Business, 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 the Windows Store for Business.
5	Create an administrator for the Windows Store for Business.

Configure BlackBerry UEM to synchronize with the Windows Store for Business

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

1. Log in to the BlackBerry UEM management console.
2. Go to **Settings > App management > Windows 10 apps**.
3. Enter the information you copied from the Azure portal when you created the enterprise application in Azure.
 - **Client ID:** The Application ID generated by the Azure application registration
 - **Client key:** The client secret generated by the Azure application registration
 - **OAuth 2.0 token endpoint:** The tenant specific OAuth endpoint URL for requesting authentication tokens
 - **Username:** The administrator username for BlackBerry UEM to access Intune
 - **Password:** The password for the username
4. Click **Next**.

After you finish: [Create an administrator for the Windows Store for Business](#).

Create an administrator for the Windows Store for Business

To manage Windows 10 apps on devices, you must create an app catalog in the Windows Store for Business and synchronize the apps with BlackBerry UEM. To create the catalog in the Windows Store for Business, you must create at least one administrator account to log in to the store.

Before you begin:

- [Create a Microsoft Azure account.](#)
 - [Create an enterprise endpoint in Azure.](#)
 - [Configure BlackBerry UEM to synchronize with the Windows Store for Business.](#)
1. In the Microsoft Azure portal, go to **Microsoft Azure > Azure Active Directory > Users and groups > All users**.
 2. Click **Add a user**.
 3. On the screen, enter the required user information.
 4. Click the arrow next to **Directory role** and select **Global administrator**, then click **OK**.
 5. Create a password or select **Show Password** and copy the generated password.
 6. Click **Create**.
 7. Click **Azure Active Directory > Enterprise applications > All applications** and select the enterprise application you created.
 8. Add the global administrator account you created as a user of the application.

Activate the app in the Windows Store for Business

Before you begin:

- [Configure BlackBerry UEM to synchronize with the Windows Store for Business.](#)
 - [Create an administrator for the Windows Store for Business](#)
1. Log in to the [Windows Store for Business](#) using the Global Admin account you created.
 2. Click **Manage > Settings > Distribute**.
 3. Click **Add Management tool**.
 4. Choose the app that you created to be the MDM tool you want to synchronize with the Windows Store for Business.
 5. Click **Activate**.

Allowing users to install online Windows 10 apps

To allow users to install online Windows 10 apps, the user must exist in your Microsoft Azure directory, and the user's email address in BlackBerry UEM must match the user's email address in Microsoft Azure AD. You can synchronize your directory to Microsoft Azure using Microsoft Azure AD Connect. For instructions, [see the Configuration content](#).

Note: To be able to send required online apps to devices, instruct your users to add their work accounts to **Accounts used by other apps** in Windows 10.

Add an app category for a Windows 10 app

After you set a category for an app, you can filter apps in the app list by category and organize the apps in the work apps list on users' devices into categories. After a Windows 10 app has been synchronized to BlackBerry UEM, you can assign an app category to it.


Before you begin: [Add a Windows 10 app to the app list](#).

1. On the menu bar, click **Apps**.
2. Click the app that you want to assign an app category to.
3. In the **Category** drop-down list, do one of the following:

Step	Description
Select a category for the app	a. In the drop-down list, select a category.
Create a category for the app	a. Type a name for the category. A "new category" message will appear in the drop-down list with the new category label beside it b. Press Enter . c. Press Enter .

4. Click **Save**.

Add a BlackBerry 10 app to the app list

1. On the menu bar, click **Apps**.
2. Click .
3. Click **BlackBerry World**.
4. In the search field, search for the app that you want to add. You can search by app name, vendor, or BlackBerry World URL.
5. In the drop-down list, select the country of the store that you want to search in.
6. Click **Search**.
7. In the search results, click **Add** to add an app.
8. To filter BlackBerry 10 apps in the app list by category, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Task	Steps
Select a category for the app	a. In the drop-down list, select a category.
Create a category for the app	a. Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside it b. Press Enter . c. Press Enter .

9. On the app information screen, click **Add**.

Adding internal apps to the app list

Internal apps include proprietary apps developed by your organization, or apps made available for your organization's exclusive use. Internal apps are not added from public app storefronts.

BlackBerry apps must be .bar files, iOS apps must be .ipa files, and Android apps must be .apk files. Internal apps must also be signed and unaltered.

Users can find internal apps on their devices as follows:

- For BlackBerry 10 devices, in the Company Apps tab in BlackBerry World for Work
- For iOS and Android devices, in the Assigned work apps list in the BlackBerry UEM Client app

For more information on BlackBerry Dynamics apps, see [Add an internal BlackBerry Dynamics app entitlement](#).

Steps to add internal apps to the app list

When you add internal apps, you perform the following actions:

Step	Action
1	Specify the shared network location for storing internal apps.
2	If the app is not a BlackBerry Dynamics app, add an internal app to the app list .
3	If the app is a BlackBerry Dynamics app, add an internal BlackBerry Dynamics app entitlement and then upload the BlackBerry Dynamics app source files .
4	If you are adding an internal app that you want to make available on Android Enterprise devices, perform the steps to host the app in Google Play or in BlackBerry UEM .

Specify the shared network location for storing internal apps

Before you add internal apps to the available app list, you must specify a shared network location to store the app source files. To make sure that internal apps remain available, this network location should have a high availability solution and be backed up regularly. Also, do not create the shared network folder in the BlackBerry UEM installation folder because it will be deleted if you upgrade BlackBerry UEM.

Before you begin:

- Create a shared network folder to store the source files for internal apps on the network that hosts BlackBerry UEM.
- Verify that the service account for the computer that hosts BlackBerry UEM has read and write access to the shared network folder.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **App management**.
3. Click **Internal app storage**.
4. In **Network location** field, type the path of the shared network folder using the following format:


`\\<computer_name>\<shared_network_folder>`

The shared network path must be typed in UNC format (for example, \\ComputerName\Applications\InternalApps).

5. Click **Save**.

Add an internal app to the app list

Before you begin: [Specify the shared network location for storing internal apps](#).

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Internal apps**.
4. Click **Browse**. Navigate to the app that you want to add or update.
5. Click **Open**.
6. Click **Add**.
7. Optionally, add a vendor name and an app description.
8. To add screen shots of the app, click **Add**. Browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
9. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

Task	Steps
Select a category for the app	<ol style="list-style-type: none">a. In the drop-down list, select a category.
Create a category for the app	<ol style="list-style-type: none">a. Type a name for the category. The "new category" will appear in the drop-down list with the new category label beside itb. Press Enter.c. Press Enter.

10. In the **App rating and review** drop-down list, perform one of the following actions. When multiple versions of the app exist, the setting specified applies to all versions of the app.
 - If you want users to rate and provide reviews of apps and see all reviews submitted by other users in your environment, select **Public mode**.
 - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
 - If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.
11. If you are adding an iOS app, perform the following actions:
 - a) In the **Supported device form factor** drop-down list, select the form factors that the app can be installed on. For example, you can prevent the app from being available in the Work Apps app for iPad.
 - b) If you want the app to be deleted from the device when the device is removed from BlackBerry UEM, select **Remove the app from the device when the device is removed from BlackBerry UEM**. This option applies only to apps with a disposition marked as required and the default installation for required apps is set to prompt once.
 - c) If you want to prevent apps on iOS devices from being backed up to the iCloud online service, select **Disable iCloud backup for the app**. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.

- d) In the **Default installation method for required apps** drop-down list, if you want users to receive one prompt to install the app on their iOS devices, select **Prompt once**. If users dismiss the prompt, they can install the app later from the Work Apps list in the BlackBerry UEM Client app or the Work Apps icon on the device.

12.If you are adding an Android app, in the **Send to** drop-down list, perform one of the following actions:

- If you want the app to be sent to all Android devices, select **All Android devices**.
- If you want the app to be sent to only Android devices that use Samsung KNOX Workspace, select **Samsung KNOX Workspace devices**.
- If you want the app to be sent only to Android Enterprise devices, select **Android devices with a work profile**.

13.To allow the app to be installed on Android Enterprise devices, select **Enable the app for work profiles**.

14.For apps that support configuration settings, an **App configuration** table is displayed. Click **+** to add an app configuration. For more information, see [Adding or changing an app configuration](#).

15.Click **Add**. If you plan to host the app in BlackBerry UEM using a .json file, copy and save the URL that is displayed.

After you finish: If you selected the **Enable the app for Android work profiles** option, complete one of the following tasks:

- [Host an internal app for Android Enterprise devices in Google Play using the .apk file](#)
- [Host an internal app for Android Enterprise devices in BlackBerry UEM using a .json file](#)

Host an internal app for Android Enterprise devices in Google Play using the .apk file

When you host an app in Google Play, you can use configuration settings to modify app behaviors and set the app as required or optional. To host an app in Google Play, you must publish the app in Google Play so that users can install the internal app on their devices.

Before you begin:

- In BlackBerry UEM, add the internal .apk file to the app list. Select the **Enable the app for Android Enterprise** option, and in the **App will be hosted by** drop-down list, click **Google Play**.
Note: You need to select **Enable the app for Android Enterprise** even if you are hosting the app for all Android devices.
- You need an account to log in to the Google Developers Console. If Android Enterprise is configured, use the same email address for the developer account that you used to set up the work profile. For each BlackBerry UEM domain you need a different developer account.

Visit <https://support.blackberry.com/community> to read article 47873 for instructions on hosting an internal app for Android Enterprise devices in BlackBerry UEM using a .apk file.

Host an internal app for Android Enterprise devices in BlackBerry UEM using a .json file

To host an internal app for Android Enterprise devices in BlackBerry UEM, you must generate a .json file for the app, upload the file to Google Play, and get the license key for the published app. Apps that are hosted in BlackBerry UEM can be set only as optional, and you cannot use configuration settings to modify app features and behaviors.

Before you begin:

- Verify that you have OpenSSL, JDK, Python 2.x, and Android Asset Packaging Tool (aapt) installed in a Path location on the computer.
- You need an account to log in to the Google Developers Console. If you configured support for Android Enterprise, use the same email address for the developer account that you used to set up Android Enterprise. For each BlackBerry UEM domain you need a different developer account.

- In BlackBerry UEM, [Add an internal app to the app list](#). Select the **Enable the app for Android Enterprise** option, and in the **App will be hosted by** drop-down list, click **BlackBerry UEM**. Copy and save the URL that is displayed in BlackBerry UEM.

Note: You need to select **Enable the app for Android Enterprise** even if you are hosting the app for all Android devices.


Visit <https://support.blackberry.com/community> to read article 47768 for instructions on hosting and updating an internal app for Android Enterprise devices in BlackBerry UEM using a .json file.

Update an internal app

When you update an internal app, the updated app will replace the app currently assigned to users and groups. BlackBerry devices update the app version automatically. Other devices may prompt the user to install the new app version.

Note: If you are updating an internal iOS app with a pre-existing app configuration, create an app configuration of the same name during the version update. BlackBerry UEM can then automatically deploy the new version to users. For more information, see [Adding or changing an app configuration](#).

Before you begin: If you are updating an app that is hosted in Google Play for Android Enterprise devices, add the updated version of the app to Google Play and wait for Google to publish the app before you update the app in BlackBerry UEM.

1. On the menu bar, click **Apps**.
2. Click on the internal app that you want to update.
3. In the top-right corner, click .
4. In the **Update internal app** dialog box, click **Browse** and navigate to the app that you want to update.
5. Click **Add** until the **Save** button appears.
6. Click **Save**.

Adding app shortcuts

You can use app shortcuts to add a customized shortcut to the device or BlackBerry Dynamics Launcher. For example, you can add a shortcut to your organization's internal website. For each app shortcut, you can configure the following attributes:


- Web address that opens when users tap the icon
- Icon and label of the shortcut
- Location to add the app shortcut (for example, the BlackBerry Dynamics Launcher)
- If the web address opens in the secure BlackBerry Access browser

Create an app shortcut

You must create an app shortcut for each shortcut that you want to display on users' devices. For devices activated with BlackBerry Dynamics, you have the option to add the shortcut to the BlackBerry Dynamics Launcher.

Before you begin:

- Verify that users are assigned an app entitlement for "Feature – BlackBerry App Store" (com.blackberry.feature.appstore).
- Verify that the image that you plan to use as the icon for the shortcut meets the following requirements:
 - The image format is .png, .jpg, or .jpeg.

- The image does not have transparent elements. Any transparent elements will display as black on the device.
 - The maximum image size is 120x120.
1. On the menu bar, click **Apps**.
 2. Click .
 3. Click **App shortcut**.
 4. Type a name and description for the app shortcut. The name is used as the label for the app shortcut.
 5. Beside the **Shortcut icon** field, click **Browse**. Locate and select an image for the app shortcut icon. The supported image formats are .png, .jpg, or .jpeg.
 6. Select the device types that you want to configure this app shortcut for.
 7. In each of the device type tabs that you selected, do any of the following:
 - To add a shortcut to a website, in the URL field, type the web address of the shortcut. The web address must begin with http:// or https://.
 8. Select the location where you want the shortcut to be added. For devices with BlackBerry Dynamics, specify whether you want the shortcut to open in the BlackBerry Access browser.
 9. Click **Add**.

Adding or changing an app configuration

App configurations allow you to preconfigure certain app settings before you assign apps to users. By preconfiguring app settings, you can make it easier for users to download, set up, and use the apps. For example, many apps require users to type a URL, an email address, or other information before they can use the app. By adding an app configuration, you can configure some of these settings in advance. You can create multiple app configurations for an app with different settings for different purposes, and rank the configurations. If an app is assigned to a user more than once with different app configurations, the app with the highest rank is applied.

In BlackBerry UEM, you can create an app configuration for the following apps:

- iOS apps (public or internal) that are developed with Managed Configuration capabilities. See [Add an iOS app to the app list](#).
- Android apps (public or internal) that are developed with Android App Restrictions capabilities. BlackBerry UEM must be configured to support Android Enterprise. See [Add an Android app to the app list if BlackBerry UEM is configured for Android Enterprise devices](#).

For information about app settings, contact the app vendor.

For more information about app configuration, visit <http://www.appconfig.org/>.

Preventing users from installing specific apps

To help prevent users from installing specific apps, you can create a list of restricted apps and use compliance profiles to enforce the restrictions. For example, you might want to prevent users from installing malicious apps or apps that require a lot of resources.

Restrict specific apps

For iOS and Android devices, you can create a compliance profile to select apps from the restricted app list and set an enforcement action such as prompting the user or deleting work data if one of these apps is installed.

For the following devices, you don't need to specify an enforcement action because users are automatically prevented from installing apps that you specify in a compliance profile:

- For Samsung KNOX devices, if a user tries to install a restricted app, the device displays a message that the app is restricted and cannot be installed. If a restricted app is already installed, it is disabled. For Samsung KNOX devices you can select an option in the compliance profile to prevent apps being installed in the personal space as well as the work space.
- For supervised iOS devices, if a user tries to install a restricted app, the app is hidden. If a restricted app is already installed, it is hidden from the user without any notification. To restrict built-in apps you must create a compliance profile and add the apps to the restricted app list in the profile. For more information, see [iOS : Compliance profile settings](#).
- For Android Enterprise devices, you don't need to create a compliance profile to restrict apps, other than system apps, because users can only install apps in the work space that you have assigned. If a restricted app is already installed on a device, it is not disabled. If you want to restrict a system app (such as calculator, clock, or camera), you must add the system app to a compliance profile to enforce the restriction.
- For BlackBerry 10 devices, you don't need to create a compliance profile to restrict apps because users can only install apps in the work space that you have assigned. If a restricted app is already installed on a device, it is not disabled.

Allow specific apps

For supervised iOS devices, you can create a compliance profile that specifies a list of allowed apps. All other apps, with the exception of the Phone and Preferences apps, are automatically disallowed and cannot be seen on the device. Apps that are already installed that are not on the allowed list are hidden from the user without any notification. The following apps are included on the allowed list by default to ensure that devices can be managed in BlackBerry UEM:

- BlackBerry UEM Client
- Web Clip icons
- BlackBerry Secure Connect Plus

Note: If the same iOS app is assigned to both the restricted list and allowed list in a compliance profile, the app is restricted.

For more information about creating compliance profiles, see [Create a compliance profile](#).

Steps to prevent users from installing specific apps

When you prevent users from installing apps, you perform the following actions:

Step	Action
1	<p>Add an app to the restricted app list.</p> <p>Note: You need to add apps to the restricted app list whether you want to select specific apps to restrict or select specific apps to allow.</p> <p>Note: This step does not apply to built-in apps for supervised iOS devices. To restrict built-in apps you must create a compliance profile and add the apps to the restricted app list in the profile. For more information, see iOS : Compliance profile settings.</p>
2	Create a compliance profile.
3	Assign the compliance profile to user accounts , user groups , or device groups .

Add an app to the restricted app list

The restricted app list is a library of apps that you can select from when you want to enforce one of the following compliance rules:

- Restricted app installed (for iOS and Android devices)
- Show only allowed apps on device (for supervised iOS devices)

1. On the menu bar, click **Apps**.
2. Click **Restricted apps**.
3. Click **+**.
4. Perform one of the following tasks:

Task	Steps
Add an iOS app to the restricted list	<ol style="list-style-type: none"> a. Click App Store. b. In the search field, search for the app that you want to add. You can search by app name, vendor, or App Store URL. c. Click Search. d. In the search results, click Add to add an app.
Add an Android app to the restricted list	<ol style="list-style-type: none"> a. Click Google Play. b. In the App name field, type the app name. c. In the App web address from Google Play field, type the web address of the app in Google Play. d. Click Add to add the app or click Add and new to add another app after you add the current one.


Managing apps on the app list

The app list contains apps that you can assign to users, user groups, and device groups. The app list includes the following information:

- App name and icon
- App vendor
- Supported device OS
- Number of applied users
- Number of devices the app is installed on
- App rating
- App source

You can click the number of applied users to display information about the installation status for the app.


You can click the number of devices the app is installed on to see a count of confirmed and unconfirmed installations. Unconfirmed installations include installations on iOS devices with the User privacy activation type because UEM can't confirm if the app is still installed on the device.

Apps listed with a lock icon  are BlackBerry Dynamics apps. For more information, see [Managing BlackBerry Dynamics apps](#).

Note: Apps assigned to users by a Microsoft Intune app protection profile don't appear in the app list.

Delete an app from the app list

When you delete an app from the app list, the app is unassigned from any users or groups that it is assigned to and it no longer appears in a device's work app catalog.

1. On the menu bar, click **Apps**.
2. Select the check box beside the apps that you want to delete from the app list.
3. Click .
4. Click **Delete**.

Change whether an app is required or optional

You can change whether an app is required or optional. The actions that occur when an app is set to required or optional depend on the type of app, the device, and the activation type.

1. On the menu bar, click **User and Devices**.
2. If the app that you want to change is assigned to a user account, in the search results, click the name of a user account.
3. If the app that you want to change is assigned to a group, in the left pane, click **Groups** to expand the list of user groups and click the name of the group.
4. In the **Groups assigned and user assigned apps** section, click the disposition for the app that you want to change.
5. In the **Disposition** drop-down list for the app, select **Optional** or **Required**.
6. Click **Assign**.

Device notifications for new and updated apps

In most cases, users receive notifications on their devices when you assign new apps, or when updates are available for internal apps. In addition to device notifications, any new or updated apps appear in the "New" list of the app catalog in the BlackBerry UEM Client or the Work Apps app.

Apps (both required and optional) appear in the "New" list in the following situations:

- An app is assigned to a user and the app is not already installed on their device
- An app is assigned to a user and is automatically installed
- An upgrade for an installed app is available
- Users have BlackBerry Access installed on their devices
- The Feature - BlackBerry App Store entitlement has been assigned to users

BlackBerry UEM will periodically resend notifications to devices if apps remain in the "New" list.

In the "New" list of apps, if a user clicks on a new app to see the app details, the app is removed from the "New" list whether or not the user installs the app. If a user clicks on an updated app, the app remains in the list until the update is installed.

For more information about app notifications, see:

- [App behavior on iOS devices](#)
- [App behavior on Android devices](#)
- [App behavior on Android Enterprise devices](#)
- [App behavior on Samsung KNOX devices](#)

App behavior on iOS devices

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have added it to the BlackBerry Dynamics Launcher.

For iOS devices activated with MDM controls and User privacy, the following behavior occurs:

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	<p>If apps are already installed, user is prompted to allow UEM to manage the apps.</p> <p>On supervised devices, apps are installed automatically.</p> <p>On non-supervised devices activated with MDM controls, user is prompted to install apps.</p> <p>On devices activated with User privacy, user is not prompted to install apps. User must go to the app catalog to install the required apps.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	<p>iTunes notifies users of available updates.</p> <p>Apps are removed from the "New/Updated" list when the user updates the app. (can take up to one hour)</p> <p>For devices that do not have access to iTunes, users are not notified but can download the update from the app catalog.</p>	<p>Apps are automatically removed from devices activated with MDM controls without notification.</p> <p>Apps are not removed from devices activated with User privacy.</p> <p>Apps no longer appear in the app catalog.</p>	<p>For devices activated with MDM controls, apps are removed automatically.</p> <p>For devices activated with User privacy, users are prompted to remove the apps.</p>

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with an optional disposition	<p>If app is already installed, nothing happens.</p> <p>User is notified of a change to the app catalog.</p> <p>Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed).</p> <p>Users can choose whether to install the apps.</p>	<p>iTunes notifies users of available updates.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (whether or not the app is updated).</p>	<p>Apps are automatically removed from devices activated with MDM controls without notification.</p> <p>Apps are not removed from devices activated with User privacy.</p> <p>Apps no longer appear in the app catalog.</p>	<p>For devices activated with MDM controls, apps are removed automatically.</p> <p>For devices activated with User privacy, users are prompted to remove the apps.</p>

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with a required disposition	<p>If apps are already installed, user is prompted to allow UEM to manage the apps.</p> <p>On supervised devices, apps are installed automatically.</p> <p>On non-supervised devices, users are prompted to install apps. If the user cancels the installation, they can install apps from the app catalog.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	Apps are removed from the "New/Updated" list when the user updates the app.	<p>Apps are automatically removed from devices activated with MDM controls without notification.</p> <p>Apps are not removed from devices activated with User privacy.</p> <p>Apps no longer appear in the app catalog.</p>	<p>For devices activated with MDM controls, apps are removed automatically.</p> <p>For devices activated with User privacy, users are prompted to remove the apps.</p>

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with an optional disposition	<p>If apps are already installed, nothing happens.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p>	Apps are removed from the "New/Updated" list when the user updates the app.	<p>Apps are automatically removed from devices activated with MDM controls without notification.</p> <p>Apps are not removed from devices activated with User privacy.</p> <p>Apps no longer appear in the app catalog.</p>	<p>For devices activated with MDM controls, apps are removed automatically.</p> <p>For devices activated with User privacy, users are prompted to remove the apps.</p>

App behavior on Android devices

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have added it to the BlackBerry Dynamics Launcher.

For Android devices activated with MDM controls and User privacy, the following behavior occurs:

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	<p>User is notified of a change to the app catalog.</p> <p>Apps are removed from the "New/Updated" list when the user views the details (even if the app is not installed), or when the user installs the apps.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	User is notified by Google Play.	<p>The user is prompted to remove the apps.</p> <p>Apps no longer appear in the app catalog.</p>	The user is prompted to remove the apps.
Public apps with an optional disposition	The user can choose whether to install the apps.	User is notified by Google Play.	<p>The user is prompted to remove the apps.</p> <p>Apps no longer appear in the app catalog.</p>	The user is prompted to remove the apps.
Internal apps with a required disposition	<p>User is notified of a change to the app catalog.</p> <p>Apps are installed automatically.</p> <p>Apps are removed from the "New/Updated" list when the user views the details or when the app is installed.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	<p>User is notified of a change to the app catalog.</p> <p>Updates are installed automatically.</p> <p>Apps are removed from the "New/Updated" list when the user views the details or when the app is updated.</p>	<p>The user is prompted to remove the apps.</p> <p>Apps no longer appear in the app catalog.</p>	The user is prompted to remove the apps.

App type	When apps are assigned to a user	When apps are updated	When apps are unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with an optional disposition	The user can choose whether to install the apps. Apps appear in the "New/Updated" list.	Apps appear in the "New/Updated" list.	The user is prompted to remove the apps. Apps no longer appear in the app catalog.	The user is prompted to remove the apps.

App behavior on Android Enterprise devices

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have added it to the BlackBerry Dynamics Launcher.

For devices activated with "Work and personal - user privacy," "Work and personal - full control," or "Work space only," the following behavior occurs:

App type	When the app is assigned to a user	When apps are updated	When the app is unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	Apps are automatically installed.	Apps are automatically updated.	Apps are automatically removed from the device.	The work profile and assigned work apps are removed from the device.
Public apps with an optional disposition	The user can choose whether to install the apps. Apps appear in Google Play for Work.	Google Play for Work notifies users about updates.	Apps are automatically removed from the device.	The work profile and assigned work apps are removed from the device.
Internal apps with a required disposition hosted in BlackBerry UEM	Supported only for Work space only devices. Apps are automatically installed.	Supported only for Work space only devices. Apps are automatically installed.	Apps are automatically removed from the device.	Apps are automatically removed from the device.

App type	When the app is assigned to a user	When apps are updated	When the app is unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with an optional disposition hosted in BlackBerry UEM	The user can choose whether to install the apps. Apps appear in Google Play for Work.	Google Play for Work notifies users about updates.	Apps are automatically removed from the device.	The work profile and assigned work apps are removed from the device.
Internal apps with a required disposition hosted in Google Play	Apps are automatically installed on the device.	Google Play for Work notifies users about updates.	Apps are automatically removed from the device.	The work profile and assigned work apps are removed from the device.
Internal apps with an optional disposition hosted in Google Play	The user can choose whether to install the apps. Apps appear in Google Play for Work.	Google Play for Work notifies users about updates.	Apps are automatically removed from the device.	The work profile and assigned work apps are removed from the device.

App behavior on Samsung KNOX devices

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have added it to the BlackBerry Dynamics Launcher.

For Samsung KNOX devices activated with "MDM controls," the following behavior occurs:

App type	When the app is assigned to a user	When apps are updated	When the app is unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	<p>The user is prompted to install the apps.</p> <p>Assigned apps are shown in the BlackBerry UEM Client. When the user clicks the install button, Google Play opens and the app is installed from there.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	<p>Google Play notifies users of updates.</p> <p>App appears in the "New/Updates" list.</p>	The user is prompted to uninstall the apps.	The user is prompted to uninstall assigned work apps
Public apps with an optional disposition	<p>The user can choose whether to install the apps.</p> <p>Assigned apps are shown in the BlackBerry UEM Client. When the user clicks the install button, Google Play opens and apps are installed from there.</p>	<p>Google Play notifies users of updates.</p> <p>App appears in the "New/Updates" list.</p>	The user is prompted to uninstall the apps.	The user is prompted to uninstall assigned work apps
Internal apps with a required disposition	Apps are automatically installed on devices. The user cannot uninstall the apps.	Apps are updated automatically.	Apps are automatically removed from the device.	Apps are automatically removed from the device.
Internal apps with an optional disposition	<p>User can choose whether to install the apps.</p> <p>User installs apps from the BlackBerry UEM Client.</p>	<p>User can choose whether to update the apps.</p> <p>User updates apps from the BlackBerry UEM Client.</p>	Apps are automatically removed from the device.	Apps are automatically removed from the device.

For devices activated with Work space only (Samsung KNOX), the following behavior occurs:

App type	When the app is assigned to a user	When apps are updated	When the app is unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	<p>All public apps are restricted by default in the work space.</p> <p>Assigned apps are shown in the "New/Updated" list, but they must be installed from Google Play.</p> <p>Apps are removed from the "New/Updated" list when the user views the details or when the app is updated.</p> <p>Google Play must be enabled in the IT policy that is assigned to the user.</p> <p>You can use a compliance profile to define the actions that occur if a required app is not installed.</p>	<p>Google Play notifies users of updates.</p> <p>Apps appear in the "New/Updates" list.</p> <p>Apps are removed from the "New/Updated" list when the user views the details or when the app is updated.</p>	<p>Apps are removed from the device, and can no longer be installed from Google Play.</p>	<p>The work space and all work apps are removed automatically.</p> <p>Apps are no longer automatically restricted in Google Play.</p>

App type	When the app is assigned to a user	When apps are updated	When the app is unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with an optional disposition	<p>All public apps are restricted by default in the work space.</p> <p>Assigned apps are shown in the "New/Updated" list, but they must be installed from Google Play.</p> <p>Apps are removed from the "New/Updated" list when the user views the details or when the app is updated.</p> <p>Google Play must be enabled in the IT policy that is assigned to the user.</p>	<p>Google Play notifies users of updates.</p> <p>Apps appear in the "New/Updates" list.</p> <p>Apps are removed from the "New/Updated" list when the user views the details or when the app is updated.</p>	Apps are removed from the device, and can no longer be installed from Google Play.	<p>Apps are removed automatically.</p> <p>Apps are no longer automatically restricted in Google Play.</p>
Internal apps with a required disposition	Apps are automatically installed on devices. The user cannot uninstall the apps.	Apps are automatically updated on the device.	Apps are automatically removed from the device.	Apps are automatically removed from the device.
Internal apps with an optional disposition	<p>Users can choose whether to install the apps.</p> <p>Users install the apps from the BlackBerry UEM Client.</p>	<p>Users can choose whether to install the apps.</p> <p>Users install the apps from the BlackBerry UEM Client.</p>	Apps are automatically removed from the device.	Apps are automatically removed from the device.

For devices activated with "Work and personal - full control (Samsung KNOX)" and "User privacy (Samsung KNOX)", the following behavior occurs:

App type	When the app is assigned to a user	When apps are updated	When the app is unassigned from a user	When the device is removed from BlackBerry UEM
Public apps with a required disposition	<p>All public apps are restricted by default in the work space.</p> <p>The user is prompted to install the apps.</p> <p>Assigned apps are shown in the BlackBerry UEM Client. When the user clicks the install button, Google Play opens and the app is installed from there.</p> <p>You can use a compliance profile to define the actions that occur if required apps are not installed.</p>	Google Play sends a notification	Apps remain in the personal space but are removed from the work space.	The work space is removed and the apps remain in the personal space.
Public apps with an optional disposition	<p>All apps are restricted by default in the work space.</p> <p>Assigned apps are shown in the BlackBerry UEM Client, but they must be installed from Google Play.</p> <p>Google Play must be enabled in the IT policy that is assigned to the user.</p>	Google Play sends a notification	Apps remain in the personal space but are removed from the work space.	The work space is removed and the apps remain in the personal space.
Internal apps with a required disposition	Apps are automatically installed in the work space. The user cannot uninstall the apps.	Updates are automatically installed.	Apps are automatically removed from the device.	The work space is removed and the apps remain in the personal space.

App type	When the app is assigned to a user	When apps are updated	When the app is unassigned from a user	When the device is removed from BlackBerry UEM
Internal apps with an optional disposition	<p>Users can choose whether to install the apps.</p> <p>Users install apps from the BlackBerry UEM Client and apps are installed in the work space.</p>	<p>Users can choose whether to update the apps.</p> <p>Users update app from the BlackBerry UEM Client.</p>	Apps are automatically removed from the device.	The work space is removed and the apps remain in the personal space.

App behavior on Windows 10 devices

App type	Behavior when apps are assigned to a user	Behavior when apps are unassigned from a user	Behavior when devices are removed from BlackBerry UEM
Offline Windows Store apps with a required disposition	The apps are automatically installed on devices. Users cannot uninstall the apps.	The apps are automatically removed from devices.	The apps are automatically removed from devices.
Online Windows Store apps with a required disposition	The apps are automatically installed on devices. Users cannot uninstall the apps.	The apps are automatically removed from devices.	The apps are automatically removed from devices.
Offline Windows Store apps with an optional disposition	<p>Users can choose whether to install the apps.</p> <p>For offline apps, users install the app from the BlackBerry UEM App Catalog.</p> <p>Not supported on Windows 10 Mobile devices.</p>	Users are not prompted to uninstall the apps.	Users are not prompted to uninstall assigned apps.

App type	Behavior when apps are assigned to a user	Behavior when apps are unassigned from a user	Behavior when devices are removed from BlackBerry UEM
Online Windows Store apps with an optional disposition	<p>Users can choose whether to install the apps.</p> <p>For online apps, users install the app from the Windows Store app on their devices.</p> <p>Not supported on Windows 10 Mobile devices.</p>	Users are not prompted to uninstall the apps.	Users are not prompted to uninstall the apps.
Internal apps with a required disposition	Not supported	Not supported	Not supported
Internal apps with an optional disposition	Not supported	Not supported	Not supported

App behavior on BlackBerry devices

For BlackBerry devices activated with Work and personal - Corporate (Work space only) or Work and personal - Regulated, the following occurs:

App type	Behavior when apps are assigned to a user	Behavior when apps are unassigned from a user	Behavior when the device is removed from BlackBerry UEM
Public apps with a required disposition	Not supported.	Not supported.	Not supported.
Public apps with an optional disposition	<p>The user can choose whether to install the apps.</p> <p>The apps appear in the Public Apps tab in BlackBerry World for Work.</p>	The user is prompted to uninstall the apps.	The work space and all work apps are removed automatically.
Internal apps with a required disposition	<p>The apps are automatically installed on devices.</p> <p>The user cannot uninstall the apps.</p>	The apps are automatically removed from the device.	The work space and all work apps are removed automatically.

App type	Behavior when apps are assigned to a user	Behavior when apps are unassigned from a user	Behavior when the device is removed from BlackBerry UEM
Internal apps with an optional disposition	<p>The apps are automatically installed on devices.</p> <p>The user cannot uninstall the apps.</p>	The apps are automatically removed from the device.	The work space and all work apps are removed automatically.



Managing app groups

App groups allow you to create a collection of apps that can be assigned to users, user groups, or device groups. Grouping apps helps to increase efficiency and consistency when managing apps. For example, you can use app groups to group the same app for multiple device types, or to group apps for users with the same role in your organization.

BlackBerry UEM provides a preconfigured app groups called "Recommended apps for Android devices with a work profile" and "BlackBerry Productivity Suite".

Create an app group

Before you begin: Add the apps to the app list.

1. On the menu bar, click **Apps > App groups**.
2. Click .
3. Type a name and description for the app group.
4. Click .
5. Search for and select the apps that you want to add.
6. For iOS and Android apps, if there is an available app configuration, select the app configuration to assign to the app.
7. If you are adding iOS apps, perform one of the following tasks:

Task	Steps
If you have not added a VPP account	a. Click Add .

Task	Steps
If you have added at least one VPP account	<ol style="list-style-type: none"> Click Add. 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. If you assign a license to the app, in the App licenses drop-down list, select the VPP account to associate with the app. In the Assign license to drop-down list, assign the license to the User or Device. If the App license drop-down list is not specified, the App license to drop-down list is not available. Click Add, then click Add again. <p>Users must follow the instructions on their devices to enroll in your organization's VPP 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.</p>

- Click **Add**, then click **Add** again.

Edit an app group

- On the menu bar, click **Apps > App groups**.
- Click the app group that you want to edit.
- Make the necessary edits.
- Click **Save**.

View the status of apps and app groups assigned to user accounts

- On the menu bar, click **Apps**.
- Under **Applied users** for the app or app group that you want to view, click the number.
- Click **Assigned to x users** to view the user accounts that this app is assigned to.
- View the **Assignment** column to verify whether the app or app group was assigned directly to the user account or to a group.
- View the **Status** column to verify whether an app is installed on a device. The following are the possible statuses:
 - Installed:** The app is installed on the user's device. For iOS devices with the User privacy activation type, this status indicates only that installation was initiated. BlackBerry UEM can't confirm if the app remains installed on the device.
 - Not installed:** The app has not been installed on the user's device or has been removed from the user's device.
 - Cannot be installed:** The app is not supported on the user's device.
 - Not supported:** The device's OS does not support this app.


View which apps are assigned to user groups

1. On the menu bar, click **Apps**.
2. Under **Assigned to users** for the app that you want to view, click the number.
3. Click the **Assigned to x groups** to view the user groups that this app is assigned to.

Viewing and customizing the apps list


You can customize the apps list and select the information to display. You can use filters to view only the information that is relevant to your task. You can select and reorder the columns in the apps list. You can add and remove columns in the apps list. You can use one or multiple filters to control the apps that are displayed. For example, you can filter the app list by app type, OS, category, secured type, and app rating.


Select the information to display in the apps list

1. On the menu bar, click **Apps > All apps**.
2. Click  at the top of the apps list and perform any of the following actions:
 - Click **Select all** or select the check box for each column that you want to display.
 - Clear the check box for each column that you want to remove.
 - Click **Reset** to return to the default selections.
3. To reorder the columns, click a column header and drag it to the left or right.

Filter the app list

When you turn on multiple selection, you can select multiple filters before you apply them, and you can select multiple filters in each category. When you turn off multiple selection, each filter is applied when you select it, and you can select only one filter in each category.

1. On the menu bar, click **Apps > All apps**.
2. Click  to turn multiple selection on or off.
3. Under **Filters**, expand one or more categories.

Each category includes only filters that display results and each filter indicates the number of results to display when you apply it.
4. Perform one of the following actions:
 - If you turned on multiple selection, select the check box for each filter that you want to apply and click **Submit**.
 - If you turned off multiple selection, click the filter that you want to apply.
5. Optionally, in the right pane, click **Clear all** or click  for each filter that you want to remove.

Update the app list


You can update the app list to make sure that you have the latest information about BlackBerry 10, iOS, Windows 10, and BlackBerry Dynamics apps in the apps list.

If you have configured BlackBerry UEM to support Android Enterprise devices, you can also update app information for Android apps. If you added Android apps before you configured support for Android Enterprise or

if app permissions have changed, you must update the app information to make them available on Android Enterprise devices. This also applies if you make any changes to your Android Enterprise configuration.

If you have not configured support for Android Enterprise, information about Google Play apps must be updated manually. 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.


If you configured your Apple VPP account to automatically update the app information for iOS apps, you must update the apps in the app list.

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

Update app permissions for Android Enterprise apps

If you do not accept app permissions on behalf of users, the app cannot be assigned to Android Enterprise devices. You must accept app permissions when you add the app to the app list, and you might have to reaccept them later if the permissions for the app change.

Apps can also be unapproved or deleted from the Google Play console but still appear as if they are available in BlackBerry UEM. You must update the app information in BlackBerry UEM to synchronize permissions with Google Play.

1. On the menu bar, click **Apps**.
2. Click .
3. In the app list, apps with permission changes are shown with a caution icon and a status message. The following statuses may occur after you update the app list. Perform one of the following tasks to resolve the issue:

Status	Steps
Reaccept app permissions	<p>The app permissions have changed in the Google Play console. To be able to manage the app, you must reaccept the app permissions. To reaccept the permissions, complete the following steps:</p> <ol style="list-style-type: none">a. Click Reaccept app permissions.b. Click Accept.
Delete app from BlackBerry UEM	<p>The app was unapproved from the Google Play console but was not removed from BlackBerry UEM. If you want to continue to manage this app on devices, you must approve the app in the Google Play console. If you no longer want to manage the app, complete the following steps:</p> <ol style="list-style-type: none">a. Click Delete app from BlackBerry UEM.b. Click Delete.

Status	Steps
Approve app in Google Play	<p>The app was unapproved in the Google Play console. To be able to manage the app, you must approve the app in the Google Play console. To approve the app, complete the following steps:</p> <ol style="list-style-type: none"> Click Approve app in Google Play. Accept the app permissions. Click Accept.
App was added in Google Play and is being added to BlackBerry UEM	<p>Apps that have been added to the Google Play for Work console, but not to BlackBerry UEM, are automatically synchronized to BlackBerry UEM when you update the app list. You do not have to perform any actions.</p>

4. Click **Close**.

Accept app permissions for Android Enterprise apps

You must accept the app permissions before you can manage apps on Android Enterprise devices. You can accept app permissions when you add the app to BlackBerry UEM or after you update the app list. If you do not accept the app permissions in these cases, you can also accept the app permissions from the app information screen. Apps that have permission changes are shown with a caution icon in the apps list.

Before you begin:

- Update the app list.
1. On the menu bar, click **Apps**.
 2. Click the app that you want to accept the permissions for.
 3. Click **Accept app permissions** to accept the app permissions.
 4. Select **Accept**.
 5. Click **Save**.

Managing apps protected by 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.

For iOS and Android devices, if you want to use 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](#) in the Configuration content.

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.

Note: If you update the app protection policy in Intune, the changes are not synchronized with BlackBerry UEM. After you create an app protection profile in UEM, do not update the corresponding policy from within Intune.

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 a Microsoft Intune app protection profile](#).

Before you configure BlackBerry UEM to synchronize with Microsoft Intune, you must connect BlackBerry UEM to Microsoft Azure and create an enterprise endpoint in Azure. For more information, [see the Configuration content](#).

Configure BlackBerry UEM to synchronize with Microsoft Intune

1. Log in to the BlackBerry UEM management console.
2. Go to **Settings > External Integration > Microsoft Intune**.
3. Enter the information you copied from the Azure portal when you created the enterprise application in Azure.
 - **Azure Tenant ID:** The ID of the Azure Active Directory where you registered the application
 - **Client ID:** The application ID generated by the Azure application registration
 - **Client key:** The client secret generated by the Azure application registration
4. Select one of the following authentications options:
 - **Client credentials authentication:** Enter username and password. The username is the administrator account that BlackBerry UEM uses to access Intune. Visit <https://support.blackberry.com/community> to read article 50341 for information on the permissions required for the Intune administrator account. The password is the password for the Intune administrator account.
 - **Modern authentication:** The **Reply URL** field is automatically populated with the web address of BlackBerry UEM management console. This option provides increased security.
5. Click **Next**.

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

Create a Microsoft Intune app protection profile

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.

Before you begin:

- [Configure the connection between BlackBerry UEM and 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, ensure the Microsoft Company Portal app is installed on devices. 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. Configure the appropriate values for each device type.
6. Click **Add**.

After you finish: Assign the Intune app protection profile to a directory-linked group.

Microsoft Intune app protection profile settings

[Microsoft Intune app protection profiles](#) are supported on the following device types:

- iOS
- Android

Common: Microsoft Intune app protection profile settings

Intune app protection profile setting	Description
Interoperability	
Enable interoperability between Intune and Dynamics apps	<p>This setting specifies whether BlackBerry Dynamics apps can interact with Intune-managed apps, such as Microsoft Office 365 apps, on the device.</p> <p>To allow interoperability between BlackBerry Dynamics apps and Intune-managed apps, BlackBerry Enterprise BRIDGE must be installed on users' devices.</p> <p>For more information see the BlackBerry Enterprise BRIDGE Administration Guide</p>
Data relocation	

Intune app protection profile setting	Description
Interoperability	
Allow app to transfer data to other apps	<p>This setting specifies the apps Intune-managed apps can send data to.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Policy managed apps: This option allows data to be transferred only to other apps that are managed by Intune. • All apps • None
Allow app to receive data from other apps	<p>This setting specifies the apps that apps managed by the app protection policy can receive data from.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Policy managed apps: This option allows data to be transferred only from other apps that are managed by Intune. • All apps • None
Prevent "Save as"	<p>This setting specifies whether the "Save As" option is enabled for apps.</p> <p>If you select this setting, you can allow using the "Save As" option to save work data only to one or more of the following locations:</p> <ul style="list-style-type: none"> • Local storage • OneDrive for Business • SharePoint
Restrict cut, copy, and paste with other apps	<p>This setting specifies how cut, copy, and paste operations can be used with the app.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Blocked: This option prevents cut, copy, and paste operations between this app and other apps. • Policy managed apps: This option allows cut, copy, and paste operations between the app and other apps that are managed by Intune. • Policy managed apps with paste in: This option allows pasting data from any app, but data cut or copied from a policy-managed app can be pasted only to other apps that are managed by Intune. • Any app: This option allows cut, copy, and paste operations between all apps on the device.
Restrict web content to display in the managed browser	<p>This setting specifies whether web links in apps must be opened in a browser managed by Intune.</p>
Disable contact sync	<p>This setting specifies whether the app can save contacts to the native Contacts app on the device.</p>

Intune app protection profile setting	Description
Interoperability	
Disable printing	This setting specifies whether the app can print data.
Access	
Require corporate credentials for access	<p>This setting specifies whether users must use their organization credentials to access the app.</p> <p>If this rule is selected, it takes precedence over requirements for a PIN or fingerprint.</p>
Block managed apps from running on jailbroken or rooted devices	This setting specifies whether apps can run on jailbroken or rooted devices.
Recheck access requirements timeout period	This setting specifies, in minutes, how often the access requirements for the app are rechecked when the app is open.
Offline grace period	This setting specifies, in minutes, how often the access requirements for the app are rechecked when the device is offline.
Offline interval before app data is wiped	This setting specifies, in days, how long a device can be offline before app data is wiped from the device.
Require PIN for access	<p>This setting specifies whether users must enter a PIN to access the app. If this option is selected, the user is prompted to provide a PIN the first time they run the app.</p> <p>If the "Require corporate credentials for access" setting is selected, it takes precedence over this rule.</p>
Number of attempts before PIN reset	This setting specifies the number of PIN entry attempts that can be made before the user must reset the PIN.
Allow simple PIN	This setting specifies whether users can use simple PIN sequences such as 1234 or 1111.
PIN length	This setting specifies the minimum number of digits in the PIN.
Allow fingerprint instead of PIN	This setting specifies whether users can use a fingerprint instead of a PIN to access the app.
Disable app PIN when device PIN is managed	<p>This setting specifies whether the app prompts for the PIN when the device is required to have a password.</p> <p>If this setting is selected, the app PIN is not requested on Android devices if the UEM IT policy for the device requires a password. To disable the app PIN on iOS devices, the device PIN must be required by Intune.</p>

iOS: Microsoft Intune app protection profile settings

Intune app protection profile setting	Description
Encrypt app data	<p>This setting specifies when app data is encrypted.</p> <p>Possible values:</p> <ul style="list-style-type: none"> When device is locked: This option encrypts all app data when the device is locked. When device is locked and files are open: This option encrypts app data when the device is locked. Data in open files is not encrypted After device restart: This option encrypts app data when the device is restarted until the device is unlocked for the first time. Use device settings: This option encrypts app data according to the default settings on the device. This option requires users to set a password on the device.
Prevent iTunes and iCloud	This setting specifies whether app data can be backed up to iTunes or iCloud.
App package IDs	This setting specifies the package IDs of the apps that this profile applies to. You can enter the package ID or select from the list of available Intune-managed apps.
Require minimum iOS operating system	Select this setting to specify a minimum iOS version to use this app. If the iOS version on the device does not meet the requirement, the user can't use the app. You can specify a single decimal point (for example, 12.0).
Require minimum iOS operating system (Warning only)	Select this setting to specify a minimum recommended iOS version to use this app. If the iOS version on the device does not meet the requirement, the user receives a notification that can be dismissed. You can specify a single decimal point (for example, 12.0).
Require minimum app version	<p>Select this setting to specify a minimum app version to use this app. If the app version on the device does not meet the requirement, the user can't use the app. You can specify a single decimal point (for example, 4.2).</p> <p>Because different apps usually have distinct versioning schemes, if you want to specify a minimum app version, you should create a separate profile for each app.</p>
Require minimum app version (Warning only)	<p>Select this setting to specify a minimum recommended app version to use this app. If the app version on the device does not meet the requirement, the user receives a notification that can be dismissed. You can specify a single decimal point (for example, 4.2).</p> <p>Because different apps usually have distinct versioning schemes, if you want to specify a minimum app version, you should create a separate profile for each app.</p>

Android: Microsoft Intune app protection profile settings

Intune app protection profile setting	Description
Encrypt app data	This setting specifies whether app data is encrypted. If you select this rule, app data is encrypted synchronously during all file input and output tasks.
Prevent Android backups	This setting specifies whether app data can be backed up to the Android Backup Service.
Block screen capture and Android Assistant	This setting specifies whether screen capture and Android Assistant app scanning capabilities are allowed when using a protected app. This setting is supported by Android 6.0 and later.
App package IDs	This setting specifies the package IDs of the apps that this profile applies to. You can enter the package ID or select from the list of available Intune-managed apps.
Require minimum Android version	<p>Select this setting to specify a minimum Android version to use this app. If the Android version on the device does not meet the requirement, the user can't use the app.</p> <p>You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).</p>
Require minimum Android version (Warning only)	<p>Select this setting to specify a minimum recommended Android version to use this app. If the Android version on the device does not meet the requirement, the user receives a notification that can be dismissed.</p> <p>You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).</p>
Require minimum Android patch version	<p>Select this setting to specify a minimum Android patch version to use this app. If the Android patch version on the device does not meet the requirement, the user can't use the app.</p> <p>Specify the version using the date format YYYY-MM-DD.</p>
Require minimum Android patch version (Warning only)	<p>Select this setting to specify a minimum recommended Android patch version to use this app. If the Android patch version on the device does not meet the requirement, the user receives a notification that can be dismissed.</p> <p>Specify the version using the date format YYYY-MM-DD.</p>
Require minimum app version	<p>Select this setting to specify a minimum app version to use this app. If the app version on the device does not meet the requirement, the user can't use the app.</p> <p>You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).</p> <p>Because different apps usually have distinct versioning schemes, if you want to specify a minimum app version, you should create a separate profile for each app.</p>

Intune app protection profile setting	Description
Require minimum app version (Warning only)	<p>Select this setting to specify a minimum recommended app version to use this app. If the app version on the device does not meet the requirement, the user receives a notification that can be dismissed.</p> <p>You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).</p> <p>Because different apps usually have distinct versioning schemes, if you want to specify a minimum app version, you should create a separate profile for each app.</p>

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**.

Managing Apple VPP accounts


The Apple Volume Purchase Program (VPP) allows you to buy, distribute, and update installed iOS apps in bulk. You can link Apple VPP accounts to BlackBerry UEM so that you can distribute purchased licenses for iOS apps associated with the VPP accounts.

Add an Apple VPP account

To see how to add an Apple VPP account, [visit our YouTube channel](#).


1. On the menu bar, click **Apps > iOS app licenses**.
2. Click **Add an Apple VPP account**.
3. Type a name and the account holder information for the VPP account.
4. In the **VPP service token** field, copy and paste the 64-bit code from the .vpp token file. This is the file that the VPP account holder downloaded from the VPP store.
5. Click **Next**.
6. Select the apps that you want to add to the app list. If an app has already been added to the app list, you cannot select it.
7. If you want the apps to be updated automatically when an updated version is available on BlackBerry UEM, select **Automatically update the app when a new version is available**. This setting applies to all VPP apps for this VPP account. You can edit this setting later.
8. If you want the apps to be removed from devices when the apps are deleted from BlackBerry UEM, select **Remove the app from the device when the device is removed from the system**.
9. To prevent apps on iOS devices from being backed up to the iCloud online service, select **Disable iCloud backup for the app**. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.
10. In the **Default installation method** drop-down list, perform one of the following actions:
 - Select **Prompt once** if you want users to receive one prompt to install the apps on their iOS devices. If users dismiss the prompt, they can install the apps later from the Work Apps list in the BlackBerry UEM Client app or the Work Apps icon on the device.
 - Select **No prompt**. Users are not notified. They can install the apps from the Work Apps list in the BlackBerry UEM Client app or the Work Apps icon on the device.
11. Click **Add**.

Edit an Apple VPP account

1. On the menu bar, click **Apps > iOS app licenses**.
2. Click .
3. Edit any of the following VPP account information settings:
 - VPP account name
 - VPP account holder information
 - VPP service token
 - Automatically update the app when a new version is available.
4. Click **Save**.


Update Apple VPP account information

When the App Licenses page is opened, the most current licensing information is synced automatically from the Apple VPP servers. If necessary, you can also manually update the licensing information that you have added to BlackBerry UEM.

1. On the menu bar, click **Apps**.
2. Click **iOS app licenses**.
3. Click .

Delete an Apple VPP account

Before you begin: Remove apps that have associated licenses from users before deleting the VPP account.

1. On the menu bar, click **Apps**.
2. Click **iOS app licenses**.
3. Click .
4. Click **Delete**.

Assigning Apple VPP licenses to devices

You can assign Apple Volume Purchase Program (VPP) licenses to iOS devices. Assigning VPP licenses to devices instead of to users simplifies the process for users because they no longer require an Apple ID to install apps. Additionally, apps do not appear in users' purchase history and app installs. When you change the existing assignment type for an app from user assigned to device assigned, the user must re-install the app before the new assignment is applied and displayed in the BlackBerry UEM management console.

Assigning VPP licenses to devices is supported only on iOS devices that are activated with MDM controls.

You can assign VPP licenses to devices when apps are added to any of the following groups and accounts:

- User accounts
- App groups
- User groups

Assigning VPP licenses to device groups is not supported.

View Apple VPP license assignment

You can view the status of the Apple VPP license assignment in your domain.

1. On the menu bar, click **Apps > iOS app licenses**.
2. If you have more than one Apple VPP account, click the VPP account that you want to view the VPP license assignment for.

For each iOS app in the domain, you can view the following VPP license information:

- The number of available VPP licenses
- The number of used VPP licenses

3. In the **Used licenses** column for the app, click the used licenses link.

For the specified app, you can view the following app license assignment information:

- The usernames that the app is licensed to
- If the app license is assigned to a user account or a device
- If a VPP license is used or not used
- If the app is installed or not installed

4. Click **Close**.

Limiting devices to a single app

On supervised iOS devices, Android devices managed using Samsung KNOX MDM, or Windows 10 Enterprise and Windows 10 Education devices managed using MDM, you can use an app lock mode profile to limit devices to run only one app. For example, you can limit access to a single app for training purposes or for point-of-sales demonstrations. On iOS devices, the home button on a device is disabled and the device automatically opens the app when the user wakes up the device or restarts it.

Create an app lock mode profile

Specify a single app to run on devices and select the device settings that you want to enable for the user. For supervised iOS devices, you can select an app in the app list, specify the bundle ID of the app, or select a built-in app. For Android devices that are managed using Samsung KNOX MDM, specify the app package identifier that you want to set as the home screen. For Windows 10 devices managed using MDM, specify the account and the Application User Model ID (AUMID) of the app. Visit docs.microsoft.com to find the AUMID.

Note: If the user does not install the app on a device, when you assign the profile to a user or user group the device is not restricted to the app.

Before you begin: For iOS devices, if you plan to use the app list to select an app, make sure that the app is available in the app list.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > App lock mode**.
3. Click **+**.
4. Type a name and description for the profile.
5. Specify the device types the profile applies to.
6. Perform one of the following tasks:

Task	Steps
Specify the app to run on iOS devices	<p>In the Specify the app to run on the device section, perform one of the following actions:</p> <ul style="list-style-type: none">• Click Add an app, and click an app in the list.• Click Specify the bundle ID of an app and type the bundle ID (for example, <code><com.company.appname></code>). Valid characters are uppercase and lowercase letters, 0 to 9, hyphen (-), and period (.).• Click Select a built-in iOS app and select an app from the drop-down list.
Specify the app to run on Android devices	<p>In the Specify the app to run on the device field, type the app package identifier of the app that you want to set as the home screen.</p>
Specify the app to run on Windows 10 devices	<ul style="list-style-type: none">• In the Account field, type a user account name that includes the domain name and user name. For a local user, use the device name in place of the domain name.• In the Application User Model ID field, type the AUMID of the app (for example, the AUMID for the Calculator app is <code>Microsoft.WindowsCalculator_8wekyb3d8bbwe!App</code>).

7. For iOS and Android devices, in the **Administrator-enabled settings**, select the options that you want to enable for the user when using the app.
8. For iOS devices, in the **User-enabled settings**, select the options that the user can enable.
9. Click **Add**.

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

Viewing personal app lists

By default, BlackBerry UEM receives a list of the personal apps that are installed on devices activated with a supported activation type.

In the BlackBerry UEM management console you can view the list of personal apps on the device details page for a specific user account, or on the Personal apps page for all user accounts. See [View the personal apps list in the management console](#).

Note: You can also view apps that were installed on devices before they were activated as KNOX Workspace only devices.

Viewing a list of personal apps is not supported for devices that are activated with the following activation types:

- iOS and Android: User privacy
- Android: Work and personal - user privacy
- Samsung KNOX: Work and personal - user privacy - (Samsung KNOX)
- BlackBerry 10: Work and personal - Corporate
- iOS and Android: Device registration for BlackBerry 2FA only

To turn off the collection of personal apps for all activation types, you must deselect the "Allow personal app collection" setting in the Enterprise Management Agent profile. For more information, see [Turn off personal apps collection](#).

View the personal apps list in the management console

You can view the following information about apps that are installed in the user's personal space:

- App name
- App version
- OS the app supports
- Number of user accounts that have the app installed


Before you begin: Create an activation profile with an activation type that supports BlackBerry UEM receiving a list of apps that are installed in the user's personal space and assign it to users or groups.

1. On the menu bar, click **Apps > Personal apps**.
2. In the **App name** column for the app, click the app name.
For the specified app, you can view the corresponding app details on the public app storefront, when applicable.
3. In the **Installed #** column for the app, click the installed number.
For the specified app, you can view the user account and the device that the app is installed on.

Turn off personal apps collection

By default, BlackBerry UEM receives a list of the personal apps that are installed on devices activated with a supported activation type. You can turn off personal apps collection for all activation types.

1. On the menu bar, click **Polices and Profiles**.
2. Expand **Enterprise Management Agent**.
3. Click the name of the profile that you want to change.

4. Click .
5. Clear the **Allow personal app collection** check box for each device type.
6. Click **Save**.

Rating and reviewing apps

You can specify whether users in your organization can rate and provide reviews of iOS, Android, and Windows 10 apps and see reviews provided by other users for internal custom apps or apps that are added to the BlackBerry UEM app list and downloaded from public app storefronts. Ratings and reviews submitted for apps cannot be seen by users outside your environment. Reviews can contain a maximum of 1000 characters.

Users can rate an app without providing a review, but they must rate the app when they provide a review. Ratings and reviews that are submitted by users are saved to and viewable in the BlackBerry UEM console in near real-time. You can view the average rating of an app, the number of reviews submitted, and read the individual reviews for the app. You can also delete ratings and reviews as required.

When you add multiple versions of a custom app to BlackBerry UEM and enable app rating and review for one version of the app, the setting specified applies to all versions of the custom app. The average rating and review count and app rating and reviews submitted for different versions of the custom app display the same information for each version.

By default, new apps added to the app list in the BlackBerry UEM management console allow users to rate the app, provide reviews of the app, and see reviews provided by other users in your organization. By default, app rating and review is disabled for existing apps, but you can enable this feature as required. When app rating and review is enabled for an app, the permission applies to any version of the app that is added to BlackBerry UEM.

Rating and reviewing apps is not supported on the following devices:

- BlackBerry 10 devices
- Android Enterprise devices

Enable or disable app ratings and reviews for all apps

You can enable or disable app ratings and reviews for all apps that you have added to BlackBerry UEM and configure the level of interaction that a user can have with the reviews and ratings.

Note: App rating and review settings are applied only to apps that you add to BlackBerry UEM after the settings are saved.

1. On the menu bar, click **Settings > App management**.
2. Click **Ratings and reviews**.
3. To enable app ratings and reviews, select **Enable app ratings and reviews**.
 - If you want users to rate and provide reviews for the app, as well as read reviews submitted by other users in your environment, select **Public mode**.
 - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
 - If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.
4. To disable app ratings and reviews, clear **Enable app ratings and reviews**.
5. Click **Save**.

Enable app ratings and reviews for existing apps

When you specify whether users can rate an app, provide reviews of an app, and see reviews provided by other users, the permission specified applies to all version of the app.

1. On the menu bar, click **Apps**.
2. Click an app.
3. On the **Settings** tab, in the **App rating and review** drop-down list, perform one of the following actions:
 - If you want users to rate and provide reviews for the app, as well as read reviews submitted by other users in your environment, select **Public mode**.
 - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
 - If you don't want users to rate or provide reviews of apps or see reviews provided by other users, select **Disabled**.
4. Click **Save**.


View app reviews in the management console

You can view the overall average rating for an app and individual ratings and reviews provided by users of an app.

1. On the menu, click **Apps**.
2. Optional, click the **App rating** column to order apps enabled for rating and reviewing.
Apps enabled for rating and review appear in the following order:
 - a. Apps with ratings and reviews
 - b. Apps without ratings and reviews
 - c. App rating is disabled
 - d. Apps that don't support ratings and reviews
3. Click an app.
4. Click the **<review number> reviews** tab.


Specify app rating and review settings for multiple apps

When you specify whether users can rate an app, provide reviews of an app, and see reviews provided by other users, the permission specified applies to all version of the app.

1. On the menu, click **Apps**.
2. Perform one of the following actions:
 - Select the check box at the top of the apps list to select all apps.
 - Select the check box for each app that you want to enable the app and rating review for.
3. Click the .
4. Select one of the following permissions:
 - If you want users to rate and provide a review for the app, as well as read reviews submitted by other users in your environment, select **Public mode**.
 - If you want users to only rate and provide reviews of apps, select **Private mode**. Users cannot see reviews provided by other users. You can see reviews in the BlackBerry UEM management console.
 - If you don't want users to rate or provide reviews of apps, or see reviews provided by other users, select **Disabled**.
5. Click **Save**.

Delete app ratings and reviews

You can delete app ratings and reviews as required.

1. On the menu, click **Apps**.
2. Optional, click the **App rating** column to order apps enabled for rating and reviewing.
3. Click an app enabled for rating and review.
4. In the **App details** screen, click the *<review number>* **reviews** tab.
5. Click **Select all** or select the check box beside each review that you want to delete.
6. Click .
7. Click **Remove**.
8. Click **Save**.

Configure the layout of apps on iOS devices

You can control the order of apps that display a user's iOS device. This profile can be used only with supervised devices.

1. On the menu bar, click **Policies and profiles**.
2. Click **Custom > Home screen layout**.
3. Click **+**.
4. In the **Type of app** list, select the type of app that you want to drag and drop onto the screen (for example, Built-in apps).
5. Drag and drop the icons from the App list to the home screen.
6. Click **Add**.

Managing notifications for apps on iOS devices

You can use per-app notification profiles to configure the notification settings for system apps and apps that you manage using BlackBerry UEM. Per-app notification profiles are supported for supervised iOS devices.

Note: You must assign a per-app notification profile to user accounts after the affected apps have already been installed on users' devices. If the profile is applied before the affected apps are installed, users may not be able to turn on notifications for the apps.

Create a per-app notification profile

Before you begin: Verify that the apps that you want to configure notification settings for are already installed on users' devices before you assign the per-app notification profile. If the profile is applied to devices before the affected apps are installed, users may not be able to turn on notifications for the apps.

1. On the menu bar, click **Policies and profiles**.
2. Click **Custom > Per-app notification**.
3. Click **+**.
4. Type a name and description for the profile.
5. In the **Per-app notification settings** section, click **+**. Perform one of the following actions to specify the app that you want to configure notification settings for:
 - To select the app from the managed app list, click **Select apps from the app list**. Search for and select the app.
 - To specify the app by its package ID, click **Add an app package ID**. Type the app name and package ID.
6. Click **Next**.
7. Click **Enable critical alert** if you want critical alerts to override your organization's do not disturb profile and notification settings. This setting applies only to iOS 12.0 and later devices.
8. In the **Notification** drop-down list, click **Enabled**.
9. Select any of the following notification options:
 - **Show in notification center**
 - **Show in lock screen**
10. In the **Notification alert type** drop-down list, select one of the following options:
 - **None:** Device users do not receive notification alerts.
 - **Banner:** Device users receive notification alerts in the banner.
 - **Modal alert:** Device users receive modal notification alerts.
11. Select any of the following notification alert options:
 - **Enable badges:** Specify whether the app displays a badge.
 - **Enable sounds:** Specify whether the app makes a sound.
 - **Show in CarPlay:** Specify whether notifications are displayed in CarPlay. This setting applies only to iOS 12.0 and later devices.
12. Click **Save**.
13. Repeat steps 4 to 9 to add additional per-app notifications.
14. Click **Add**.

After you finish:

- To edit the notification settings for an app, in the **Per-app notification settings** section, click the notification setting for the app and change the settings as necessary.
- If you created more than one per-app notification profile, [rank the profiles](#).

Managing the Work Apps icon for iOS devices

When users activate iOS devices with the MDM controls activation type, a Work Apps icon is displayed on the device. Users can tap the icon to see work apps that have been assigned to them, and they can install or update the apps as required.

You can customize the appearance of the Work Apps icon by selecting an image and name for the icon. The default name for the Work Apps icon is "Work Apps" and the default icon displays a BlackBerry logo.

Customize the Work Apps icon

When you customize the Work Apps icon, the icon is updated on all activated iOS devices.

Note: This feature is not supported on devices activated with the User privacy activation type.

Before you begin: Verify that the image you plan to use for the Work Apps icon meets the following requirements:

- Image format must be .png, .jpg, or .jpeg.
 - Avoid using .png images that have transparent elements. The transparent elements display as black on the device.
 - For suggested image sizes, visit developer.apple.com to see Icon and Image Sizes.
1. On the menu bar, click **Settings**.
 2. In the left pane, expand **App management**.
 3. Click **Work Apps app for iOS**.
 4. In the **Name** field, type a name for the custom icon. The name appears on the device just under the icon.
 5. Click **Browse**. Locate and select an image for the Work Apps icon. The supported image formats are .png, .jpg, or .jpeg.
 6. Select **Display the Work Apps app in full screen mode** to let users toggle the Work Apps icon from regular to full screen mode.
 7. Click **Save**.

Disable the Work Apps app for iOS

If users are accessing their work apps catalog from the BlackBerry Dynamics Launcher, you can disable the Work Apps app.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **App management**.
3. Click **Work Apps for iOS**.
4. Click **Disable Work Apps app**.

Set the organization name for BlackBerry World

You can add your organization's name to the BlackBerry World for Work corporate app storefront.

1. On the menu bar, click **Settings**.
2. Expand **App management** and click **BlackBerry World for Work**.
3. In **Organization name**, type the name of your organization.
4. Click **Save**.

Managing apps on BlackBerry OS devices

If the BlackBerry UEM domain supports BlackBerry OS (version 5.0 to 7.1) devices, you can use the management console to install and manage the BlackBerry Device Software and BlackBerry Java Applications on BlackBerry OS devices.

To send BlackBerry Java Applications to BlackBerry OS devices, you must first add the apps to the shared network folder. You can use the shared network folder to store and manage all versions of the BlackBerry Java Applications that you want to install on, update on, or remove from devices.

In the management console, you create software configurations to specify the versions of the BlackBerry Device Software and BlackBerry Java Applications that you want to install on, update on, or remove from BlackBerry OS devices. You also use software configurations to specify which apps are required, optional, or not permitted. When you create a software configuration, you must also specify whether users can install apps that are not listed in the software configuration.

When you add a BlackBerry Java Application to a software configuration, you must assign an application control policy to the app to specify what resources the app can access. You can use default application control policies or you can create and use custom application control policies. If you permit users to install unlisted applications, you must create an application control policy for unlisted applications that specifies what resources the applications can access.

When you assign a software configuration to a user group or individual user accounts, the management console creates a deployment job to install the BlackBerry Device Software and BlackBerry Java Applications on devices and to apply application control policies to the devices.

For more information about installing and managing the BlackBerry Device Software on BlackBerry OS devices, [download the BlackBerry Device Software Update Guide](#).

Preparing to distribute BlackBerry Java Applications

To send a BlackBerry Java Application to BlackBerry OS (version 5.0 to 7.1) devices, the application developer must create a .zip file that contains the necessary application files and an .alx file that contains information about the app. If a directory structure is described in the .alx file, that directory structure must be represented in the .zip file.

Before you distribute BlackBerry Java Applications, you must specify a shared network folder for BlackBerry Java Applications using the management console. For more information, refer to [Specify the shared network location for storing internal apps](#).

After you add an app to the shared network folder, you can add the app to a software configuration, specify whether the app is required, optional, or not permitted on BlackBerry OS devices, and assign an application control policy to the app to control the access permissions for the app. You assign software configurations to user accounts to install or upgrade BlackBerry Java Applications on BlackBerry devices, or to remove BlackBerry Java Applications from BlackBerry OS devices.

Add a BlackBerry Java Application to the shared network folder

To send a BlackBerry Java Application to BlackBerry OS (version 5.0 to 7.1) devices, you must first add the BlackBerry Java Application bundle to the shared network location. To send an updated version of a BlackBerry Java Application to BlackBerry OS devices, you must first add the updated bundle to the application repository. For more information on setting up a shared network folder, see [Specify the shared network location for storing internal apps](#).

1. On the menu bar, click **BlackBerry OS Settings**.

2. Click **Add or update applications**.
3. In the **Application location** section, click **Browse**. Navigate to the BlackBerry Java Application bundle that you want to add to, or update in, the application repository.
4. Click **Next**.
5. Click **Add application**.

Specify keywords for a BlackBerry Java Application

You can specify keywords for a BlackBerry Java Application. You can use the keywords to search for the application in the application repository.

1. On the menu bar, click **BlackBerry OS Settings**.
2. Click **Manage applications**.
3. Search for an application.
4. In the search results, click the name of an application.
5. Click **Edit application**.
6. In the **Application keywords** field, type a keyword.
7. Click the **Add** icon.
8. Repeat steps 6 and 7 for each keyword that you want to add.
9. Click **Save all**.

Configuring application control policies

When you add a BlackBerry Java Application to a software configuration so that you can install the app on BlackBerry OS (version 5.0 to 7.1) devices, you must specify an application control policy that you want to apply to the BlackBerry Java Application. Application control policies control the data and APIs that BlackBerry Java Applications can access on BlackBerry OS devices, and the external data sources and network connections that BlackBerry Java Applications can access.

BlackBerry UEM includes a standard application control policy for BlackBerry Java Applications that you classify as required, optional, or not permitted. You can change the default settings of the standard application control policies or create custom application control policies for a BlackBerry Java Application.

For more information about configuring settings for application control policy rules, [download the BES5 Policy Reference Guide](#).

Standard application control policies

BlackBerry UEM includes the following standard application control policies for BlackBerry OS (version 5.0 to 7.1) devices.

Application control policy	Description
Standard Required	When you apply the application control policy to a BlackBerry Java Application, rule settings require that the BlackBerry Java Application be installed and permitted to run on BlackBerry OS devices. BlackBerry OS devices install the app automatically.

Application control policy	Description
Standard Optional	When you apply the application control policy to a BlackBerry Java Application, rule settings make the BlackBerry Java Application optional on the BlackBerry OS device. Users can install and run the BlackBerry Java Application on their BlackBerry OS devices.
Standard Disallowed	When you apply the application control policy to a BlackBerry Java Application, rule settings prevent users from installing the BlackBerry Java Application on BlackBerry OS devices. Users cannot install and run the BlackBerry Java Application on their BlackBerry OS devices.

Change a standard application control policy

When you add a BlackBerry Java Application to a software configuration, you must assign an application control policy to the BlackBerry Java Application. Based on the requirements of your organization's environment, you can change the default settings for the standard application control policies.

1. On the menu bar, click **BlackBerry OS Settings**.
2. Click **Manage default application control policies**.
3. Click the standard application control policy that you want to change.
4. Click **Edit application control policy**.
5. On the **Access settings** tab, in the **Settings** section, change the settings for the standard application control policy.
6. Click **Save all**.

Create custom application control policies for a BlackBerry Java Application

After you add a BlackBerry Java Application to the shared network folder, you can configure the app to use the standard application control policies, or you can create custom application control policies for the app. If you want a BlackBerry Java Application to use custom application control policies, you must create the custom application control policies before you add the app to a software configuration. When you add the app to a software configuration, you can select which custom application control policy you want to apply to the app.

If you add the BlackBerry Java Application to multiple software configurations and you assign different custom application control policies to the BlackBerry Java Application in the different software configurations, you must set the priority for the custom application control policies. This priority determines which custom application control policy the BlackBerry Policy Service applies if you assign multiple software configurations to a user account.

1. On the menu bar, click **BlackBerry OS Settings**.
2. Click **Manage applications**.
3. Search for a BlackBerry Java Application.
4. In the search results, click a BlackBerry Java Application.
5. In the **Application versions** section, click the version of the application that you want to create a custom application control policy for.
6. Click **Edit application**.
7. On the **Application control policies** tab, in the **Settings** section, select the **Use custom application control policies** option.
8. Perform any of the following tasks:

Task	Steps
Create an application control policy for required BlackBerry Java Applications	<ol style="list-style-type: none"> In the Required application name field, type a name for the application control policy. In the Settings section, configure the settings for the application control policy. Click the Add icon. Repeat steps a to c for each application control policy that you want to create.
Create an application control policy for optional BlackBerry Java Applications	<ol style="list-style-type: none"> In the Optional application name field, type a name for the application control policy. In the Settings section, configure the settings for the application control policy. Click the Add icon. Repeat steps 1 to 3 for each application control policy that you want to create.
Create an application control policy for BlackBerry Java Applications that are not permitted.	<ol style="list-style-type: none"> In the Disallowed application name field, type a name for the application control policy. Click the Add icon.

9. If necessary, in each section, click the up and down arrows to set the priority for the application control policies.

10. Click **Save all**.

IT policy rules ranking on BlackBerry OS devices

IT policy rule settings override application control policy rule settings. For example, if you change the Allow Internal Connections IT policy rule to No for BlackBerry OS (version 5.0 to 7.1) devices, and if the devices have an application control policy set that allows a specific app to make internal connections, the app cannot make internal connections.

The device revokes an application control policy and resets if the permissions of the app it is applied to become more restrictive. Devices permit users to make app permissions more restrictive, but not less restrictive, than the permissions that you specify.

Application control policies for unlisted applications

When you create a software configuration and assign it to user accounts so that you can send BlackBerry Device Software, BlackBerry Java Applications, and standard application settings to BlackBerry OS (version 5.0 to 7.1) devices, you must configure whether the software configuration permits users to install and use apps that are not included in the software configuration (also known as unlisted applications). When you configure whether unlisted applications are permitted and optional or not permitted on BlackBerry OS devices, you must assign an application control policy for unlisted applications to the software configuration.

An application control policy for unlisted applications determines what unlisted applications are permitted on BlackBerry OS devices and what data the unlisted applications can access on BlackBerry OS devices. There are two standard application control policies for unlisted applications: one for unlisted applications that are optional, and one for unlisted applications that are not permitted. You can change the default settings of the standard

application control policy for unlisted applications that are optional, or you can create custom application control policies for unlisted applications that are optional.

Change the standard application control policy for unlisted applications that are optional

1. On the menu bar, click **BlackBerry OS Settings**.
2. Expand **Software**.
3. Click **Manage application control policies for unlisted applications**.
4. Click the **Standard Unlisted Optional** application control policy.
5. Click **Edit application control policy**.
6. On the **Access settings** tab, in the **Settings** section, configure the settings for the application control policy.
7. Click **Save all**.

Create an application control policy for unlisted applications

There are two default application control policies for unlisted applications: one for unlisted applications that you permit on BlackBerry OS (version 5.0 to 7.1) devices, and one for unlisted applications that you do not permit on BlackBerry OS devices. You can also create custom application control policies for unlisted applications that are optional.

1. On the menu bar, click **BlackBerry OS Settings**.
2. Expand **Software**.
3. Click **Create an application control policy for unlisted applications**.
4. In the **Application control policy information** section, in the **Name** field, type a name for the application control policy for unlisted applications.
5. Click **Save**.
6. On the **BlackBerry solution management** menu, click **Manage application control policies for unlisted applications**.
7. Click the application control policy that you created.
8. Click **Edit application control policy**.
9. On the **Access settings** tab, in the **Settings** section, configure the settings for the application control policy.
10. Click **Save all**.

Configure the priority of application control policies for unlisted applications

You can assign multiple software configurations to user accounts. You can assign different application control policies for unlisted applications to different software configurations. You must configure the priority of the different application control policies for unlisted applications so that the BlackBerry Policy Service can determine which application control policies to apply to user accounts when you assign multiple software configurations to user accounts.

1. On the menu bar, click **BlackBerry OS Settings**.
2. Expand **Software**.
3. Click **Manage application control policies for unlisted applications**.
4. Click **Set priority of application control policies for unlisted applications**.
5. Click the up and down arrows to set the priority of application control policies for unlisted applications.
6. Click **Save**.

Creating software configurations

You can use software configurations to perform the following actions on BlackBerry OS (version 5.0 to 7.1) devices:

- Assign application control policies to BlackBerry Java Applications to control application permissions and the data that the applications can access
- Specify that a BlackBerry Java Application is not permitted
- Specify whether BlackBerry Java Applications that you do not include in the software configuration are permitted or not permitted
- Configure the access permissions for BlackBerry Java Applications that you do not include in the software configuration
- Install or upgrade the BlackBerry Device Software over the wireless network or using the BlackBerry Web Desktop Manager
- Specify standard application settings

Steps to create and assign a software configuration

When you create and assign a software configuration, you perform the following actions:

Step	Action
1	Create and share a network folder.
2	Add the applications.
3	If necessary, create a custom application control policy.
4	Create a software configuration.
5	Add software to the software configuration.
6	Assign the software configuration to a user account or user group .

Create a software configuration

1. On the menu bar, click **BlackBerry OS Settings**.
2. Expand **Software**.
3. Click **Create a software configuration**.
4. In the **Configuration information** section, in the **Name** field, type a name for the software configuration.
5. In the **Disposition for unlisted applications** drop-down list, perform one of the following actions:
 - To permit users to install applications that are not included in the software configuration on their BlackBerry OS devices, click **Optional**.

- To prevent users from installing applications that are not included in the software configuration on their BlackBerry OS devices, click **Disallowed**.
6. In the **Application control policy for unlisted applications** drop-down list, click the application control policy for unlisted applications that you want to assign to the software configuration.
 7. Click **Save**.

After you finish: Add BlackBerry Device Software configurations and BlackBerry Java Applications to the software configuration.

Add a BlackBerry Java Application to a software configuration

You must add a BlackBerry Java Application to a software configuration and assign the software configuration to user accounts to install the BlackBerry Java Application on BlackBerry OS (version 5.0 to 7.1) devices over the wireless network. To upgrade an app, you must add the new version of the app to the appropriate software configuration. BlackBerry UEM upgrades the app that is on BlackBerry OS devices to the new version.

1. On the menu bar, click **BlackBerry OS Settings**.
2. Expand **Software**.
3. Click **Manage software configurations**.
4. Click the software configuration that you want to add a BlackBerry Java Application to.
5. Click **Edit software configuration**.
6. On the **Applications** tab, click **Add applications to software configuration**.
7. Search for the BlackBerry Java Applications that you want to add to the software configuration.
8. In the search results, select a BlackBerry Java Application that you want to add to the software configuration.
9. In the **Disposition** drop-down list for the BlackBerry Java Application, perform one of the following actions:
 - To install the BlackBerry Java Application automatically on BlackBerry OS devices, and to prevent users from removing the application, click **Required**.
 - To permit users to install and remove the BlackBerry Java Application, click **Optional**.
 - To prevent users from installing a BlackBerry Java Application on BlackBerry OS devices, click **Disallowed**.
10. In the **Application data** section, in the **Application control policy** drop-down list, click an application control policy to apply to the BlackBerry Java Application.
11. If necessary, in the **Deployment** drop-down list, perform one of the following actions:
 - To install the application on BlackBerry OS devices over the wireless network, click **Wireless**.
 - To install the application on BlackBerry OS devices using a USB connection to the user's computer and the BlackBerry Web Desktop Manager, click **Wired**.
12. Repeat steps 6 to 10 for each BlackBerry Java Application that you want to add to the software configuration.
13. Click **Add to software configuration**.
14. Click **Save all**.

Install BlackBerry Java Applications on a BlackBerry OS device at a central computer

If you do not want to install BlackBerry Java Applications on a BlackBerry OS (version 5.0 to 7.1) device over the wireless network, and you do not want the user to install the BlackBerry Java Applications using the BlackBerry Web Desktop Manager or BlackBerry Desktop Software, you can install the BlackBerry Java Applications on a BlackBerry OS device by connecting the BlackBerry OS device to a central computer that can access BlackBerry UEM.

Before you begin:

- Assign a software configuration with the necessary BlackBerry Java Applications to the appropriate user account.
 - To permit the management console to connect to a BlackBerry OS device that is attached to the computer that hosts the BlackBerry UEM management console by a USB connection, add the web address of the management console to the list of trusted web sites in the web browser. Log in to the management console again.
 - Verify that the central computer can access the management console.
 - Connect the BlackBerry OS device that is associated with the user account to the central computer.
1. On the menu bar, click **BlackBerry OS Settings**.
 2. Expand **Attached devices**.
 3. Click **Device software**.
 4. Click **Automatic installation of applications on the BlackBerry device**.
 5. Complete the instructions on the screen.

View the users that have a BlackBerry Java Application installed on their BlackBerry OS devices

1. On the menu bar, click **BlackBerry OS Settings**.
2. Expand **Software > Applications**.
3. Click **Manage applications**.
4. Search for an app.
5. In the search results, click the name of an app.
6. In the **Application versions** section, click a version of the app.
7. Click **View users with application**.
8. Search for users that are associated with BlackBerry OS devices that you installed the BlackBerry Java Application on.

Reconciliation rules for conflicting settings in software configurations

If you assign multiple software configurations to user accounts or user groups, the multiple software configurations might contain conflicting settings. For example, you might specify that a BlackBerry Java Application is required in a software configuration that you assign to a user account, but you might also specify that the same application is not permitted in a software configuration that you assign to a user group that the user account belongs to. Conflicts can occur when you assign multiple BlackBerry Java Applications, application control policies, application control policies for unlisted applications, BlackBerry Device Software, and the standard application settings in BlackBerry Device Software configurations.

BlackBerry UEM uses predefined reconciliation rules to resolve conflicting settings in multiple software configurations, and to determine which applications, software, and settings are installed on or applied to a BlackBerry OS (version 5.0 to 7.1) device. BlackBerry UEM resolves conflicting settings as an asynchronous background activity. You can view the outcome of the reconciliation activities, reconciliation errors, and the applications, software, and settings that BlackBerry UEM installed on or applied to a BlackBerry OS device.

BlackBerry UEM might have to reconcile software configuration settings that conflict if you perform any of the following actions:

- Activate a device
- Assign a new BlackBerry OS device or PIN to a user
- Add a user account to or remove a user account from a group
- Add a group to or remove a group from another group
- Add an app to or remove an app from a software configuration
- Change the settings for an app in a software configuration
- Change the settings for an application control policy
- Change the ranking for application control policies
- Install a new version of the BlackBerry Device Software on a BlackBerry OS device
- Add a BlackBerry Device Software configuration to or remove a BlackBerry Device Software configuration from a software configuration
- Change a BlackBerry Device Software configuration
- Change the standard application settings in a BlackBerry Device Software configuration

Reconciliation rules: BlackBerry Java Applications

Scenario	Rule
Multiple software configurations are assigned to a user account or the groups the user belongs to. Multiple BlackBerry Java Applications are contained in each software configuration.	The BlackBerry Java Applications in each software configuration are installed on the BlackBerry OS (version 5.0 to 7.1) device. If the BlackBerry Device Software does not support a specific BlackBerry Java Application, the application is not installed on the BlackBerry OS device.
Multiple software configurations that contain different versions of the same BlackBerry Java Application are assigned to a user account or the groups the user belongs to.	<p>When different versions of an app exist in the software configurations that are assigned to a user account, the latest version of the application that is supported by the BlackBerry Device Software is installed on the BlackBerry OS device. For example, if a software configuration with version 1.0 of an application is assigned to a user account, and another software configuration with version 2.0 of the application is assigned to a user account, version 2.0 of the application is installed on the BlackBerry OS device.</p> <p>The version of a BlackBerry Java Application that is in a software configuration that is assigned to a user account takes precedence over the version of a BlackBerry Java Application that is in a software configuration that is assigned to a group. For example, if version 1.0 of an application is in a software configuration that is assigned to a user account, and version 2.0 of an application is in a software configuration that is assigned to a group that the user belongs to, version 1.0 of the application is installed on the BlackBerry OS device.</p>

Scenario	Rule
<p>Multiple software configurations that contain the same BlackBerry Java Application are assigned to a user account or the groups the user belongs to. The disposition of the BlackBerry Java Application (required, optional, or disallowed) is different in each software configuration. The deployment method (wired or over the wireless network) for the application is different in each software configuration.</p>	<p>The disposition specified for an application in a software configuration that is assigned to a user account takes precedence over the disposition of the same application in any software configuration that is assigned to a group. If the application has different dispositions in multiple software configurations that are assigned at the same level (either to the user account or groups), the required disposition takes precedence over the optional disposition, and the optional disposition takes precedence over the disallowed disposition.</p> <p>BlackBerry UEM resolves the deployment method after resolving the disposition of an app. The deployment method specified for an app in a software configuration that is assigned to a user account takes precedence over the deployment method for the same application in any software configuration that is assigned to a group. The wireless setting takes precedence over the wired setting.</p>
<p>One or more software configurations that include BlackBerry Java Apps are assigned to a user account or the groups the user belongs to, but a limited amount of available memory remains on the BlackBerry OS device.</p>	<p>BlackBerry UEM checks the amount of available memory on the BlackBerry OS device after resolving application conflicts (for example, resolving conflicting disposition and deployment settings) and before installing a BlackBerry Java Application. If there is not enough memory available on the BlackBerry OS device to support the application, the application is not installed.</p> <p>Depending on the amount of available memory, applications are installed in the following order:</p> <ol style="list-style-type: none"> 1. Required apps that are configured for wireless deployment 2. Required apps that are configured for wired deployment 3. Optional apps that are configured for wireless deployment 4. Optional apps that are configured for wired deployment

Scenario	Rule
A software configuration is assigned to a user account and it contains a BlackBerry Java Application that has a dependency on another BlackBerry Java Application.	<p>If a BlackBerry Java Application in a software configuration has a dependency on another application, and the other application is not included in a software configuration that is assigned to the user account or a group that the user belongs to, the application is not installed on the BlackBerry OS device.</p> <p>If a BlackBerry Java Application in a software configuration has a dependency on another app, and the dependent app is included in a software configuration that is assigned to the user account or a group the user belongs to, the dependent app is installed first. If the dependent app is installed successfully, the app with the dependency is then installed.</p>
A software configuration is assigned to a user account and it contains a BlackBerry Java Application that has a dependency on another BlackBerry Java Application. The dependent application is not supported on the BlackBerry OS device.	If a dependent application is not supported by the BlackBerry OS device or was not installed successfully on the BlackBerry OS device, the application with the dependency is not installed on the user's BlackBerry OS device.
Multiple BlackBerry Java Applications have a circular dependency (for example, application A is dependent on application B, application B is dependent on application C, and application C is dependent on application A) and are included in the same application bundle. The application bundle is added to the application repository. The apps are added to a software configuration and assigned to a user account or a group the user belongs to.	If multiple BlackBerry Java Apps are included in the same application bundle and have a circular dependency, the applications are not installed on the BlackBerry OS device. If multiple apps have a circular dependency, they can only be installed if they exist in separate application bundles and are installed using wired deployment.

Reconciliation rules: BlackBerry Device Software

Scenario	Rule
A software configuration that contains BlackBerry Device Software is assigned to a user account. A software configuration that contains a different version of BlackBerry Device Software is assigned to a group that the user account belongs to.	The BlackBerry Device Software in a software configuration that is assigned to a user account takes precedence over the BlackBerry Device Software in a software configuration that is assigned to a group.

Scenario	Rule
Multiple software configurations that contain different versions of BlackBerry Device Software are assigned to a user account.	The version of the BlackBerry Device Software that is supported by the BlackBerry OS (version 5.0 to 7.1) device and by the wireless service provider, and that you ranked highest in the BlackBerry UEM management console, is installed on the BlackBerry OS device. BlackBerry UEM does not install a version of the BlackBerry Device Software if that version is ranked lower than the version of the BlackBerry Device Software that is currently installed on the BlackBerry OS device.

Reconciliation rules: Standard application settings

Scenario	Rule
A software configuration with standard application settings is assigned to a user account. A software configuration with different standard application settings is assigned to a group that the user account belongs to.	The standard application settings in a software configuration that is assigned to a user account take precedence over the standard application settings in a software configuration that is assigned to a group.
A user account belongs to multiple groups. The calendar initial view setting is configured differently in each of the software configurations that are assigned to the groups.	The calendar initial view setting that is applied to the user's BlackBerry OS (version 5.0 to 7.1) device is the lowest value that was specified in the multiple software configurations.
A user account belongs to multiple groups. The calendar keep appointments setting is configured differently in each of the software configurations that are assigned to the groups.	The calendar keep appointments setting that is applied to the user's BlackBerry OS device is the highest value that was specified in the multiple software configurations.
A user account belongs to multiple groups. The email confirm delete setting is set to Yes in one or more of the software configurations that are assigned to the groups. The setting is set to No in the remaining software configurations.	If the email confirm delete setting is set to Yes in a software configuration that is assigned to a group that the user account belongs to, the Yes setting is applied to the BlackBerry OS device.
A user account belongs to multiple groups. The email hide sent messages setting is set to Yes in one or more of the software configurations that are assigned to the groups. The setting is set to No in the remaining software configurations.	If the email hide sent messages setting is set to No in a software configuration that is assigned to a group that the user account belongs to, the No setting is applied to the BlackBerry OS device.
A user account belongs to multiple groups. The email save copy in sent folder setting is set to Yes in one or more of the software configurations that are assigned to the groups. The setting is set to No in the remaining software configurations.	If the email save copy in sent folder setting is set to Yes in a software configuration that is assigned to a group that the user account belongs to, the Yes setting is applied to the BlackBerry OS device.

Scenario	Rule
A user account belongs to multiple groups. The address book sort by setting is configured differently in each of the software configurations that are assigned to the groups.	If the address book sort by setting is configured differently in the software configurations that are assigned to the groups that the user account belongs to, the first name setting takes precedence over the last name setting, and the last name setting takes precedence over the company name setting.
A user account belongs to multiple groups. The attributes settings for the various standard application settings are configured differently in the software configurations that are assigned to the groups.	The Locked and visible setting takes precedence over the Unlocked and visible setting. The Unlocked and visible setting takes precedence over the Unlocked and hidden setting.
Standard application settings are configured in a software configuration and assigned to user accounts with BlackBerry OS devices that are running a BlackBerry Device Software version earlier than 5.0.	Standard application settings apply only to BlackBerry OS devices that are running BlackBerry Device Software version 5.0 or later.

Reconciliation rules: Application control policies

Scenario	Rule
A user is assigned multiple software configurations that each contain the same application. A different application control policy is assigned to the application in each software configuration.	<p>An application control policy for an application in a software configuration that is assigned to a user account takes precedence over an application control policy for the same application in a software configuration that is assigned to a group. The required setting takes precedence over the optional setting. The optional setting takes precedence over the disallowed setting.</p> <p>If multiple software configurations contain the same application, and each software configuration is assigned a different custom application control policy with the same disposition (for example, two custom required application control policies), the application control policy that you ranked highest in the BlackBerry UEM management console is applied to the user's BlackBerry OS (version 5.0 to 7.1) device.</p>

Reconciliation rules: Application control policies for unlisted applications

Scenario	Rule
A software configuration with a default or custom application control policy for unlisted applications is assigned to a user account. A software configuration with a different application control policy for unlisted applications is assigned to a group that the user account belongs to.	The application control policy for unlisted applications in a software configuration that is assigned to a user account takes precedence over the application control policy for unlisted applications in a software configuration that is assigned to a group.
A software configuration that defines unlisted applications as disallowed is assigned to a user account. A software configuration that defines unlisted applications as optional is also assigned to the user account.	If unlisted applications are defined as disallowed in a software configuration that is assigned to a user account, unlisted applications are not permitted on the BlackBerry OS (version 5.0 to 7.1) device.
Multiple software configurations with different application control policies for unlisted applications are assigned to a user account.	The application control policy for unlisted applications that you ranked highest in the BlackBerry UEM management console is applied to the BlackBerry OS device.

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.

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