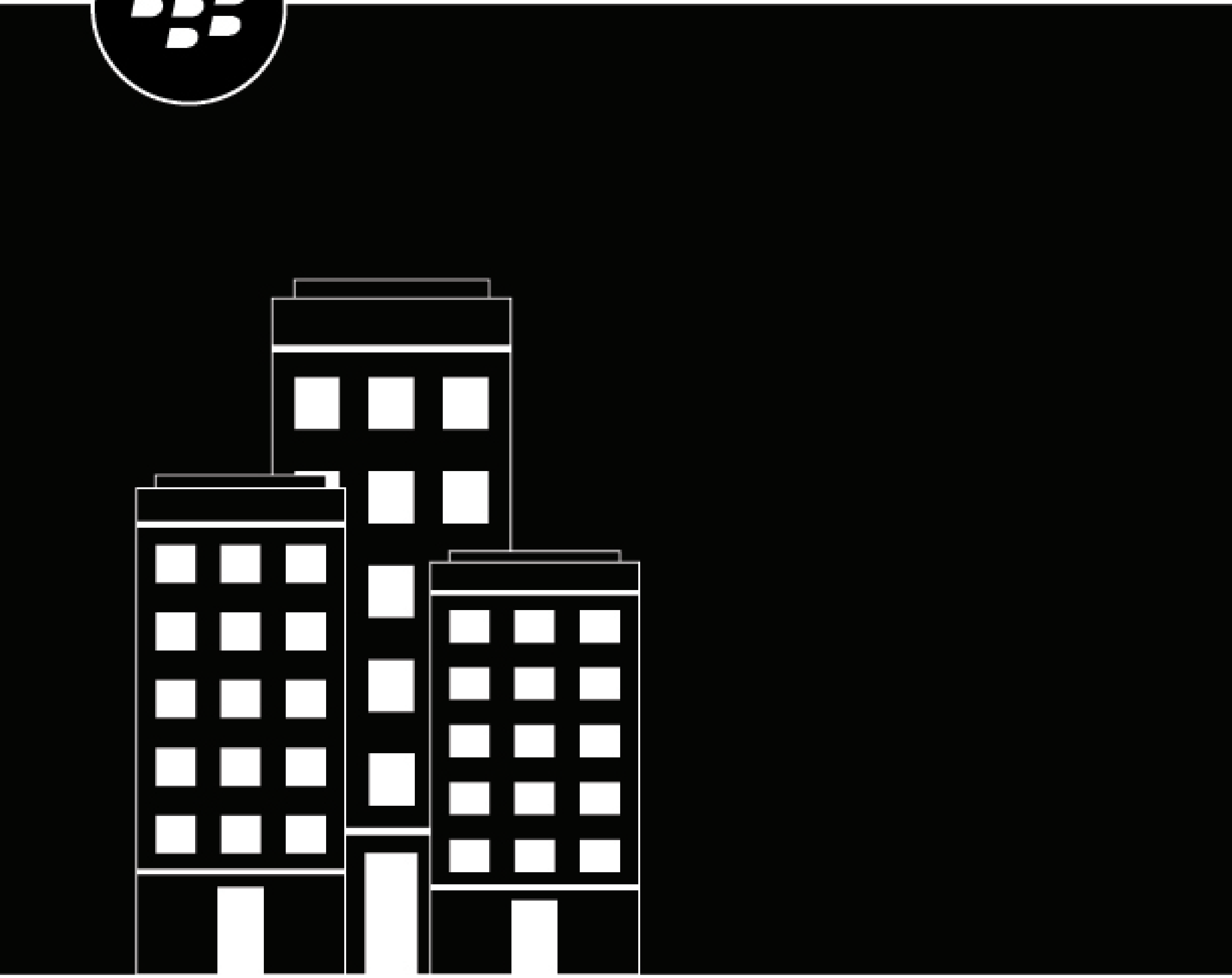

BlackBerry UEM

Managing apps

Administration

12.23

Contents

Managing apps

In BlackBerry UEM, you can create a list of apps that you can manage, deploy, and monitor on devices. Apps that are added to this list are considered to be work apps. To deploy apps to users' devices, you assign apps that are in the app list to user accounts, user groups, or device groups.

The following tables summarizes the essential tasks that you might complete when you want to manage apps for your organization.

Task	Description
Add public and internal apps to UEM.	Add apps to the apps list so that you can assign them to users' devices. You can add public apps, such as those from the App Store and Google Play store. You can also add internal apps which you upload the source files for. You can specify app configurations, which 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.
Create and manage 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.
Assign apps or app groups to user accounts, user groups, or device groups.	Assign apps or app groups so that users can install them. You can also specify whether the apps are required or optional.
Prevent users from installing specific apps.	Create a list of restricted apps to prevent users from installing them on their devices.
Create a Microsoft Intune app protection profile for apps protected by Intune.	If your organization uses Microsoft Intune for mobile management of apps such as Office 365 apps, you must create a Microsoft Intune app protection profile to assign apps protected by Intune to users instead of adding them to the app list.

Apps listed with a lock icon 🔒 are BlackBerry Dynamics apps.

Adding apps to the app list

Add apps to the app list so that you can assign them to users, user groups, and device groups. Apps listed with a lock icon 🔒 are BlackBerry Dynamics apps.

If your organization uses Microsoft Intune for mobile management of apps such as Office 365 apps, you must create a Microsoft Intune app protection profile to assign apps protected by Intune to users instead of adding them to the app list.

Adding public apps to the app list

A public app is an app that is available from the App Store and the Google Play store.

For more information on adding 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, see KB 52777.

1. In the management console, 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.	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** again.

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 but allow it for iPhone.
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" setting is set to prompt once. You set the disposition of the app when you assign the app to a user or group.
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 a prompt to install the app on their iOS devices, select **Prompt once**.
    - If you don't want users to receive a prompt, select **No prompt**.

    If users dismiss the prompt or don't receive a prompt, they can install the app later from the Work Apps screen in the BlackBerry UEM Client app or the Work Apps icon on the device. This option to prompt the user 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.	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.
Copy another app configuration.	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.	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 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 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, see KB 52777.

If 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, you must allow Google Play app management for Samsung Knox Workspace devices in the activation profile.

1. In the management console, on the menu bar, click **Apps**.
2. Click ⊞.
3. Click **Google Play**.
4. In the left navigation menu, click ▶.
5. Search for and select the app that you want to add.
6. Click **Approve**.
7. Click **Done**.
8. In the **App description** field, type a description for the app.
9. To add screen shots of the app, click **Add**. Browse to and select the screen shots (.jpg, .jpeg, .png, or .gif).
10. In the **Send to** drop-down list, do one of the following:
    - 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**.
11. For apps that support configuration settings, an **App configuration** table is displayed. If you want to create an app configuration, complete the following steps:
    a) Click + to add an app configuration.
    b) Type a name for the app configuration and specify the configuration settings to use.
    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.
12. For devices with Google Play app management, you must use the **Organize apps** feature in the **Add Android apps** dialog box to manage your Google Play store layout. 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 create or select a category for the app. Complete the following steps:
    a) Click ⊞.
    b) Click **Google Play**.
    c) Click **Organize apps** (at the bottom of the left-hand menu).
    d) Click **Create a collection**.
    e) Name the collection and click **Next**.
    f) Select the apps that you want to add to the collection.
    g) Click **Add Apps**.

h) Click **Save**.

13. 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 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**.

14. Click **Add**.

After you finish: If necessary, you can specify the update behavior for apps running in the foreground in the device SR requirements profile.

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

1. In the management console, on the menu bar, click **Apps**.
2. Click ⊞.
3. Click **Google Play**.
4. 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.
5. In the **App name** field, type the app name.
6. 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	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**.

Adding internal apps to the app list

Internal apps include proprietary apps developed by your organization and apps made available for your organization's exclusive use.

For iOS devices and for Android devices that don't allow access to Google Play in the work profile, assigned internal apps are listed in the Assigned work apps in the BlackBerry UEM Client.

For Android Enterprise devices, a list of assigned internal apps is available in Google Play in the work profile.

For more information on BlackBerry Dynamics apps, see Add an internal BlackBerry Dynamics app entitlement.

Specify the shared network location for storing internal apps

If you have an on-premises BlackBerry UEM environment, before you add internal apps to the available app list, you must specify a shared network location to store the app source files that you upload. 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. If you have BlackBerry UEM Cloud, you don't need to specify a network location for app files.

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. In the management console, 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

Use these instructions to add internal apps to the app lists for all devices. If you are managing Android Enterprise devices, see Adding internal apps for Android Enterprise and Android Management devices for the recommended method to add internal apps for those devices.

iOS apps must be .ipa files, Android apps must be .apk files, and Windows 10 apps must be .xap or .appx files. Internal apps must be signed and unaltered.

Before you begin: If you have an on-premises BlackBerry UEM environment, Specify the shared network location for storing internal apps.

1. In the management console, 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. 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 devices but allow it for iPhone.
   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" setting is set to prompt once. You set the disposition of the app when you assign the app to a user or group.
   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 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 don't receive the prompt or dismiss it, they can install the app later from the Work Apps screen in the BlackBerry UEM Client app or the Work Apps icon on the device.
10. 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**.
11. 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.	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**.

12. 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**.

13. For apps that support configuration settings, an **App configuration** table is displayed. If you want to create an app configuration, complete the following steps:
    a) Click + to add an app configuration.
    b) Type a name for the app configuration and specify the configuration settings to use.
    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.
14. Click **Add**. If you plan to host the app in BlackBerry UEM using a .json file, copy and save the URL that is displayed.

Update an internal app

When you update an internal app, the updated app replaces the app currently assigned to users and groups. Users receive a prompt on their device to install the new version of the app.

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.

If you are updating an Android Enterprise app that you added to Google Play as a private app, see Update a private app for Android Enterprise devices.

Before you begin: If you are updating an app for Android Enterprise devices that you added to Google Play using the Google Developers Console, see Add an internal Android app using the Google Developers Console to add the updated version of the app to Google Play and wait approximately 24 hours for Google to publish the app before you update the app in BlackBerry UEM using the following steps.

1. In the management console, 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 internal apps for Android Enterprise and Android Management devices

You can add internal apps for Android Enterprise and Android Management devices using the BlackBerry UEM management console and the Google Developers Console. The method you use depends on several factors.

Option	Description
Add a private app to the app list for Android Enterprise devices using the BlackBerry UEM management console. (Android Enterprise only)	Use this option to host a new internal app as a private app in Google Play. This option doesn't require you to purchase a developer account from Google. Use this method only in the following circumstances: • You are deploying Android apps only to devices with Android Enterprise activation types. If you want to make the app available to devices with other Android activation types, use the Google Developers Console. • You are adding the app to only one UEM instance or UEM Cloud tenant. If you plan to add the app to more than one instance or tenant, you can add the app for the first time using this method and use the Google Developers Console to add it to additional instances or tenants. • You are adding a new app to the list. To update an app you have already added using this method, see Update a private app for Android Enterprise devices.
Add an internal app using the Google Developers Console.	This method involves using the Google Developers Console and requires the purchase of a developer account from Google. Use this method in the following circumstances: • You want to add the app to more than one UEM instance or tenant. • You are updating an app that you have previously added using the Google Developers Console. • Your organization does not allow Google Play in the work profile. Using this method, you can upload an .apk file to be hosted in Google Play, or you can host the app locally and upload a .json file to the Google Developers Console.

Add a private app to the app list for Android Enterprise devices using the BlackBerry UEM management console

Use these instructions to add internal apps as a private app on Google Play to deploy to Android Enterprise devices.

In the app list, private apps display the 🔒 symbol and your Android Enterprise Organization Name is in the Vendor field.

Before you begin: If you have an on-premises BlackBerry UEM environment, Specify the shared network location for storing internal apps.

1. In the management console, on the menu bar, click **Apps**.
2. Click ⊞.
3. Click **Google Play**.
4. In the left navigation menu, click **Private apps**.
5. Click +.
6. In the **Title** field, type the text that will display on the device.
7. Click **Upload APK**, navigate to the app that you want to add, and click **Open**.
8. Click **Create**.

   The web app is created in Google Play and the app appears on the Private apps tab. Google Play takes several minutes to upload and verify the .apk file and notify UEM that the app is ready. When UEM receives the .apk file, it adds the app to the app list automatically.
9. In the **App description** field, type a description for the app.

10. 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.
11. If you want the app to update automatically on Android Enterprise devices, select **Automatically update app on Android Enterprise devices when update available**.
12. For apps that support configuration settings, an **App configuration** table is displayed. If you want to create an app configuration, complete the following steps:
    a) Click + to add an app configuration.
    b) Type a name for the app configuration and specify the configuration settings to use.
    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.
13. 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.	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**.

14. 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 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**.
15. Click **Add**.

After you finish: If the app is a BlackBerry Dynamics app, create a BlackBerry Dynamics app entitlement for the app and assign both the app and the entitlement to users. For more information, see Add an internal BlackBerry Dynamics app entitlement.

Update a private app for Android Enterprise devices

You can update private apps with a new version of the .apk file and update the app information in Google Play. If you are updating the app for more than one BlackBerry UEM instance or UEM Cloud tenant, you can update the app for the first instance or tenant using this method and then use the Google Developers Console to add the update to the remaining instances or tenants.

1. In the management console, on the menu bar, click **Apps**.
2. Click ▦+.
3. Click **Google Play**.
4. In the left navigation menu, click **Private apps**.
5. Click the app that you want to update.
6. Click **Edit**.

7. To replace the .apk file with an updated version, click **Edit** next to the file name and upload a new file.
8. To update the app settings in Google Play, click **Make advanced edits** and make the required changes.
9. Click **Save**.

Add an internal Android app using the Google Developers Console

You can use the Google Developers Console to upload internal apps for Android devices. You need a Google Developer account to log in to the Google Developers Console.

If you use Google Play to host the app, 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 upload an .apk file to the Google Developers Console and publish the app in Google Play so that users can install the internal app on their devices. For instructions on uploading an .apk file for Android devices in the Google Developers Console, see Google Workspace Admin Help: Manage private Android apps in Google Play. This is supported for both Android Enterprise and Android Management devices.

If you want to host internal apps for Android devices in BlackBerry UEM (not supported for Android Management devices), you must generate a .json file for the app, upload the .json file to Google Play, and get the license key for the published app. Apps that are hosted in UEM can be set only as optional and you cannot use configuration settings to modify app features and behaviors. To host the .apk file in UEM, you must meet the following requirements:

- Verify that you have OpenSSL, JDK, Python 2.x, and the Android Asset Packaging Tool (aapt) installed in a Path location on the computer hosting the app.
- In the activation profile that is assigned to the user, verify that the "Add Google Play account to work space" option is not selected.
- If you configured support for Android Enterprise, use the same email address for the developer account that you used to set up Android Enterprise.
- Apps that are hosted in UEM can be set only as optional and you cannot use configuration settings to modify app features and behaviors.
- In 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 UEM.

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

For more information, see Managed Google Play Help: Publish private apps from the Play Console.

1. In the management console, 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. 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**.

10. 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.	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**.

11. 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**.

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

a) Click + to add an app configuration.
b) Type a name for the app configuration and specify the configuration settings to use.
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.

13. 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 are updating an app that you already added, wait 24 hours and see Update an internal app to complete the process.

Add public BlackBerry Dynamics apps to the app list

Public BlackBerry Dynamics apps are automatically added to the app list if your organization has an entitlement to use them. You can obtain entitlements for BlackBerry Dynamics apps from the BlackBerry Marketplace for Enterprise Software. UEM synchronizes with the marketplace and updates the app list every 24 hours, but you can also update the app list immediately.

Note: Users should activate the apps on the same BlackBerry UEM environment that the apps are assigned from. Activating BlackBerry Dynamics apps with access keys, activation passwords, or QR codes from an external BlackBerry Dynamics environment is not supported. To use QR codes or activation passwords, the app must use BlackBerry Dynamics SDK version 8.0 or later.

1. Log in to your account at https://marketplace.blackberry.com/apps.

2. Locate the app in the BlackBerry Marketplace for Enterprise Software and request a trial. The app will be made available to your organization and can be assigned to users after the app has been synchronized to BlackBerry UEM.
3. To purchase the app, follow the instructions provided by the app developer.

Adding internal BlackBerry Dynamics apps to the app list

When you want to add internal BlackBerry Dynamics apps to the app list, you must add the entitlements and upload the source files.

You can use the source files for apps from the public Google Play store and upload them as an internal app so that users can install the apps without accessing Google Play. When you add Google Play apps as internal apps, the "Send to" and "Restricted versions" options are not supported.

For Android Enterprise activation types, when Google Play is not accessible and the "Add Google Play account to work space" option is not selected in the activation profile that is assigned to the user, only the app source files are sent to the device.

For Android Enterprise activation types, when Google Play is accessible and the "Add Google Play account to work space" option is selected in the activation profile that is assigned to the user, only the app that is published in Google Play is sent to the device. This also applies to Samsung Knox activation types with “Google Play app management for Samsung Knox Workspace devices” selected in activation profile.

Add an internal BlackBerry Dynamics app entitlement

To add an internal BlackBerry Dynamics app, you must add an entitlement for it in BlackBerry UEM. After the entitlement has been added, you can upload the app source files.

Before you begin:

- If you have UEM in an on-premises environment, Specify the shared network location for storing internal apps.
- You must have an appropriate license to be able to add an internal BlackBerry Dynamics app entitlement. For more information, see the BlackBerry Enterprise Licensing Guide.

1. In the management console, on the menu bar, click **Apps**.
2. Click ⊞.
3. Click **Internal BlackBerry Dynamics app entitlements**.
4. In the **Name** field, type the name of the app that you want to add.
5. In the **BlackBerry Dynamics entitlement ID** field, enter the entitlement ID of the app that you want to add. If you do not know the entitlement ID for the app, contact the app developer. For more information on entitlement IDs, see the BlackBerry Dynamics SDK documentation. The entitlement ID must be in the following format:
    - Reverse domain name form, for example, `com.yourcompany.appname`.
    - Cannot begin with any of the following:
        - com.blackberry
        - com.good
        - com.rim
        - net.rim
    - Cannot contain uppercase letters
    - Must conform to the <subdomain> format defined in section 2.3.1 of RFC 1035, as amended by Section 2.1 of RFC 1123.

6. In the **BlackBerry Dynamics entitlement version** field, enter the entitlement version. If you do not know they entitlement version for the app, contact the app developer. The entitlement version must be in the following format:
    - From one to four segments of digits, separated by periods, for example, 100 or 1.2.3.4.
    - No leading zeroes in the numeric segments. For example, you cannot use 0100 or 01.02.03.04.
    - The length of the numeric segments can be from one to three characters, for example, 100.200.300.400.
7. Optionally, add an app description.
8. Click **Add**.

After you finish: Do one of the following:

- If the app will be installed on Android Enterprise devices, and you want to manage the app as a private app in Google Play, Add a private app to the app list for Android Enterprise devices using the BlackBerry UEM management console.
- If the app will be installed on Android Enterprise devices and you do not want to manage the app as a private app in Google Play, Add an internal Android app using the Google Developers Console.
- For other devices in general, Upload BlackBerry Dynamics app source files.

Upload BlackBerry Dynamics app source files

After a BlackBerry Dynamics app entitlement has been created, you can upload the source files for the applicable device platforms. You do not need to upload the source files for a BlackBerry Dynamics app if it's managed in Google Play as a private app or if you added it using the Google Developers Console.

Before you begin: Add an internal BlackBerry Dynamics app entitlement.

1. In the management console, on the menu bar, click **Apps**.
2. Click the app that you want to upload source files for.
3. Click the tab for the device platform that you want to upload a source file for.
4. In the **App source file** section, click **Add**.
5. Click **Browse**. Navigate to the app that you want to add or update.
6. Click **Add**.
7. If necessary, update the app settings. For more information, see Manage settings for a BlackBerry Dynamics app.

Add an app shortcut for iOS, macOS, and Android devices

You can create an app shortcut on devices so that users can tap it quickly access a web address. Create an app shortcut for each shortcut that you want to display on users' devices.

For Android devices, you have the option specify another app to open instead of a web address.

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).

1. In the management console, 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.
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, in the **URL** field, type the web address of the shortcut. The web address must begin with http:// or https://.:
8. For iOS and iPadOS 14 and later devices, in the **Target app** field, specify an app that you want to open the URL.
9. For iOS and iPadOS 15 and later devices, specify options for the shortcut:
    a) If you want to add the shortcut to the home screen on the device, select **User's home screen**.
    b) If you want to allow the user to delete the shortcut, select **Allow user to remove app shortcut**.
    c) If you don't want the web clip to appear in a browser window, select **Open as a full screen app**.
    d) If the web clip doesn't appear in a browser window, and you don't want the browser UI to appear when the user navigates away from the web clip, select **Ignore manifest scope**.
10. Select the location where you want the shortcut to be added. If you add the shortcut to the BlackBerry Dynamics Launcher, specify whether you want the web site to open in the BlackBerry Access browser.
11. Click **Add**.

Add or update a web app for Android Enterprise and Android Management devices

Web apps are Android apps that you create using a website address (URL), icon image, and title. When a user opens a web app on their device, the URL opens in the Google Chromebrowser.

When you add a web app, the Google web app system creates an .apk file and hosts it in Google Play for users to install in the work profile. Google generates the web app app package ID, which starts with "com.google.enterprise.webapp". In the app list,Google web apps display the 🌐 symbol and your Android Enterprise Organization Name in the Vendor field.

1. In the management console, on the menu bar, click **Apps**.
2. Click ⊞.
3. Click **Google Play**.
4. In the left navigation menu, click **Web apps**.
5. Do one of the following:

Task	**Steps**
Create a web app.	**a.** Click +. **b.** In the **Title** field, type the text that will display on the device. **c.** In the **URL** field, type the web address of the shortcut. The web address begins with https://.: **d.** Select whether you want the web app to display full screen, standalone, or with minimal UI. **e.** Click **Upload icon** and browse for the icon that you want to use for the web app. **f.** Click **Create**. The web app is created in Google Play. Google Play takes several minutes to create the .apk file and send it to UEM. When UEM receives the .apk file, it adds the web app to the app list automatically. If the app is not added to the app list as expected, follow these steps to manually add it: **a.** From the Google Play screen (Apps > Add an app > Google Play > web apps icon) select the web app you created previously. **b.** Click **Select** at the bottom-right of the screen. **c.** Click **Add**. The web app displays in the Apps list.
Update a web app.	**a.** Click the web app that you want to update. **b.** Click **Edit**. **c.** Update the settings as needed. **d.** Click **Save**. The web app is created in Google Play. Google Play takes several minutes to create the .apk file and send it to UEM. When UEM receives the .apk file, it updates the app list automatically.

Managing apps on the app list

The app list contains apps that you can assign to users, user groups, and device groups. Apps assigned to users by a Microsoft Intune app protection profile don't appear in the app list.

In the app list, BlackBerry Dynamics apps have a lock icon (🔒). For more information specific to managing BlackBerry Dynamics apps, see Managing BlackBerry Dynamics apps.

From the app list, you can click an app to understand the status of apps and app groups assigned to user accounts.

You can manage apps in the apps list from the **Apps** screen.

Tab or column name	Description
Customize the app list view.	• To change the columns that you want displayed, click ⋮ at the top right and select the columns. • To rearrange the columns, you can drag the column headers to position them.
Filter the app list.	You can filter the app list from the left pane. Each category includes only filters that display results and each filter indicates the number of results that display when you apply it. • If multiple selection is turned on, select the filters that you want and click **Submit**. • If multiple selection is turned off, you apply filters one at a time cumulatively. • On the right pane, above the results, you can click ✕ for each filter that you want to remove or click **Clear all** to display all devices.
View app assignments and installation status.	**1.** Click an app that you want to view the assignments or installation status for. **2.** In the **Assigned to x users** tab, you can see the following information: • The **Feedback** column displays the date and time of the last feedback received from Android apps. The feedback that UEM receives depends on the app and may include information feedback or as the result of an error (⚠). • The **Name** column displays the username that the app is assigned to. • The **Device** column displays the name of the device that the app is assigned to. • The **Assignment** column displays whether the app was assigned directly to the user account, user group, or device group. • The **Status** column displays whether an app is installed on a device. **3.** In the **Assigned to x groups** tab you can see the user groups that the app was assigned to and the associated number of users. If you want to remove app assignments, you can select the assignments and click 👤 or 👥.

Tab or column name	Description
Status column	This column displays whether an app is installed on a device. The possible statuses are: • **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. 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.

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 you manage apps more efficiently and consistently across devices in your organization. For example, you can use app groups to assign the same group of apps 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. In the management console, 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 to the group.
   a) For iOS and Android apps, if there is an available app configuration, you can select the **App configuration** for each app.
   b) If you are using Android Enterprise and have created tracks for apps in the Google Play console, select a **Track** to assign to the app.
6. Click **Add**.
7. If you are adding iOS apps, perform one of the following tasks:

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

Task	Steps
If you have added at least one VPP account	**a.** Click **Add**. **b.** 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. **c.** If you assign a license to the app, in the **App licenses** drop-down list, select the VPP account to associate with the app. **d.** 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. **e.** Click **Add**, then click **Add** again. 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. **Note:** If you grant access to more licenses than you have available, the first users who access the available licenses can install the app.

8. Click **Add** again.

After you finish: If you want to edit an app group, click the app group that you want to edit, then save your changes.

Update the app list

You can update the app list to make sure that you have the latest app information about iOS, Windows 10, and BlackBerry Dynamics apps in the apps list. Android apps are also updated if you have configured BlackBerry UEM to support Android Enterprise devices.

Note the following:

- If you added Android apps before you configured support for Android Enterprise, or you made changes to the configuration, you must update the app information to make them available on Android Enterprise devices.
- If you have not configured support for Android Enterprise, information about Google Play apps must be updated manually.
- 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.

Updating the app information does not mean that the app is updated on a user’s device. Users receive update notifications for their work apps in the same way that they receive update notifications for their personal apps.

1. In the management console, on the menu bar, click **Apps**.
2. Click ⟳.

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. In the management console, 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, optional, or denied

You can change whether an app is required, optional, or denied (denied is an option for Android only). 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. In the management console, do one of the following:
    a) If you want to change the disposition of an app assigned to a user, on the menu bar, click **Users**.
    b) If you want to change the disposition of an app assigned to a group, on the menu bar, click **Groups**.
2. Search for and click the name of the user or group.
3. In the **Apps** or **Assigned app** section, click the **Disposition** of the appropriate app.
4. In the **Disposition** drop-down list, select the appropriate option:
    - **Required**: Install the app automatically on devices and prevent users from uninstalling the app.
    - **Optional**: Allow users to install and uninstall the app.
    - **Denied** (Android only): Prevent users from installing the app.
5. If it is a Google Play app assigned to Android Enterprise and Android Management devices, and you set the **Disposition** to required or optional, in the **Update Mode** drop-down list, click the appropriate option:
    - **Default**: When a new version of the app is available in Google Play, the device is notified. Any restrictions or conditions from an assigned device SR requirements profile are applied to the app update.
    - **High Priority**: When a new version of the app is available in Google Play, the device is notified. Any restrictions or conditions from an assigned device SR requirements profile are ignored. In larger deployments this can take up to 24 hours.
    - **Postpone**: When a new version of the app is available in Google Play, the device is notified after 90 days, then the update is applied using latest available version. Any restrictions or conditions from an assigned device SR requirements profile are applied. Note that users can manually update the app at any time.
6. If it is an Apple VPP app, and you set the **Disposition** to required or optional, in the **Update Mode** drop-down list, click the appropriate option:
    - **Default**: When a new version of the app is available, it will be pushed to devices automatically.
    - **Postpone**: When a new version of the app is available, it will not be pushed to devices automatically.
7. Click **Save**.

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.

Managing BlackBerry Dynamics apps

If your organization uses BlackBerry Dynamics apps, you must configure connectivity settings and other options that apply only to BlackBerry Dynamics apps.

For more information on configuring network communication and properties for BlackBerry Dynamics apps, see Configuring network communication and properties for BlackBerry Dynamics apps in the Configuration content.

To use BlackBerry Dynamics apps in your organization, perform the following actions:

Step	Action
1	Check BlackBerry Dynamics connectivity settings and change them if necessary.
2	Create a BlackBerry Dynamics profile or update the Default BlackBerry Dynamics profile.
3	Add BlackBerry Dynamics apps to BlackBerry UEM: • Add public BlackBerry Dynamics apps to the app list • Add an internal BlackBerry Dynamics app entitlement
4	If required, change BlackBerry Dynamics apps settings.
5	Add the work app catalog to the BlackBerry Dynamics Launcher.
6	Assign the BlackBerry Dynamics profile and BlackBerry Dynamics connectivity profile to user accounts and groups.
7	Assign BlackBerry Dynamics apps to user accounts and groups.
8	For users who want to activate BlackBerry Dynamics apps on devices without the UEM Client, generate access keys, activation passwords, and QR codes for the apps.

Setting up network connections for BlackBerry Dynamics apps

BlackBerry Dynamics connectivity profiles define the network connections, Internet domains, IP address ranges, and app servers that BlackBerry Dynamics apps can connect to. BlackBerry UEM includes a Default BlackBerry Dynamics connectivity profile with preconfigured settings. If no BlackBerry Dynamics connectivity profile is assigned to a user account or to a user group that a user belongs to, the default profile is sent to a user's devices.

UEM automatically sends a BlackBerry Dynamics connectivity profile to a device when a user activates it, when you update an assigned BlackBerry Dynamics connectivity profile, or when you assign a different BlackBerry Dynamics connectivity profile to a user account or device.

The following options allow administrators to control how BlackBerry Dynamics traffic is routed:

- BlackBerry Dynamics connectivity profile
- BlackBerry Proxy web proxy server configuration
- App-specific settings (for example, BlackBerry Access web proxy server configuration)

Before you configure routing, ensure that you have a BlackBerry Proxy server installed, that the correct ports are open, and that you have network connectivity to the BlackBerry Dynamics NOC from the BlackBerry Proxy server. To use the BlackBerry Proxy in a BlackBerry UEM Cloud environment, you must install an on-premises BlackBerry Connectivity Node.

For more information, review the following:

- Port requirements in the Planning content
- Configuring network communication and properties for BlackBerry Dynamics apps in the Configuration content
  - Sending BlackBerry Dynamics app data through an HTTP proxy in the Configuration content.
  - Methods for routing traffic for BlackBerry Dynamics apps in the Configuration content

This documentation discusses only configurations that affect overall routing. App-specific configuration may be required for apps to connect to specific servers (for example, for BlackBerry Work configured with the URL of the Microsoft Exchange Server). Review the administration documentation for each BlackBerry Dynamics app to understand which app configurations to apply.

Create a BlackBerry Dynamics connectivity profile

1. On the menu bar, click **Policies and profiles**.
2. Click **Networks and connections > BlackBerry Dynamics connectivity**.
3. Click +.
4. Type a name and description for the profile.
5. If you have previously exported BlackBerry Dynamics connectivity profile settings that you want to reuse to a .csv file, click ⇦ to import the settings.
6. Configure the appropriate values for the profile settings. For more information about each profile setting, see BlackBerry Dynamics connectivity profile settings.
7. To add an app server for a BlackBerry Dynamics app, see Add an app server to a BlackBerry Dynamics connectivity profile.
8. Click **Save**.

After you finish: If necessary, rank the profile.

BlackBerry Dynamics connectivity profile settings

BlackBerry Dynamics connectivity profiles are supported on the following device types:

- iOS
- macOS
- Android
- Windows

BlackBerry Dynamics connectivity profile setting	Description
Name	Specify a name for the BlackBerry Dynamics connectivity profile.
Description	Specify a description for the BlackBerry Dynamics connectivity profile.

BlackBerry Dynamics connectivity profile setting	Description
Infrastructure	
Route all traffic	For apps developed with a version of the BlackBerry Dynamics SDK earlier than 6.0, this setting specifies whether all BlackBerry Dynamics app data is routed through BlackBerry Proxy. This option takes precedence over other settings in the profile. If you select Route all traffic, you can specify a BlackBerry Proxy cluster to route through or select Deny to block all connections. For apps developed with BlackBerry Dynamics SDK version 6.0 and later, the "Default allowed domain route type" replaces this setting. You should select this option only if your organization uses custom or ISV apps developed with a version of BlackBerry Dynamics SDK earlier than 6.0. Recent versions of BlackBerry Dynamics apps released by BlackBerry use a version of the SDK later than 6.0. This setting is not included in BlackBerry UEM Cloud.
Allowed domains	A list of the Internet domains that your organization wants to control access to. For example, `blackberry.com` controls access to any server in the blackberry.com domain. BlackBerry Dynamics apps are allowed to connect through your organization's firewall to any server in the listed domains and their subdomains. For BlackBerry Dynamics apps running BlackBerry Dynamics SDK versions 6.0 and later, the "Default allowed domain route type" applies to all domains that aren't otherwise specified in the profile. To add a new domain to the Allowed domains list, click + and configure the settings for the domain. To remove a domain from the list, click × beside the domain that you want to remove.
Domain	Specify the Internet domains that you want to allow or deny access to. For example, `blackberry.com` allows access to any server in the blackberry.com domain. BlackBerry Dynamics apps are allowed to connect through your organization's firewall to any server in the listed domains and their subdomains.
BlackBerry Proxy cluster	Select this option to specify the BlackBerry Proxy clusters that must be used to reach the domain.
Direct	Select this option to route traffic directly from the app to the domain without going through BlackBerry Proxy. This option is supported only for apps developed with BlackBerry Dynamics SDK version 6.0 and later.
Deny	Select this option to block the app from connecting to the domain. This option is supported for apps developed with BlackBerry Dynamics SDK version 6.0 and later.
Primary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the primary route that the app uses to connect to the domain.

BlackBerry Dynamics connectivity profile setting	Description
Secondary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the backup route that the app uses to connect to the domain if the primary cluster is down.
Default domains	A list of the default allowed domains (for example, qa.blackberry.com). BlackBerry Dynamics apps may try to connect to an unqualified hostname like "portal" instead of using a fully qualified name like "portal.sales.xyzcorp.com". The domains in this list will be appended to unqualified hostnames to construct fully qualified names. To add a new domain to the Default domains list, click + and configure the settings for the domain. To remove a domain from the list, click × beside the domain that you want to remove.
Domain	Specify the domain that you want to add to the Default domains list.
Primary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the primary route the app uses to connect to the domain.
Secondary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the backup route the app uses to connect to the domain if the primary cluster is down.
Additional servers	A list of additional servers that BlackBerry Dynamics apps can connect to. Add servers to this list if you want BlackBerry Dynamics apps to connect only to certain servers and not to every server in a domain. To add a new server to the Additional servers list, click + and configure the settings for the server. To remove a server from the list, click × beside the server that you want to remove.
Server	Specify the fully qualified domain name of any additional servers that BlackBerry Dynamics apps can connect to. Add servers to this list instead of using the "Allowed Domains" list if you want BlackBerry Dynamics apps to be able to connect only to certain servers and not to every server in a domain. Servers, routing types, and BlackBerry Proxy clusters listed in this section have precedence over entries listed in the “Allowed Domains” section.
Port	Specify the port that the server uses.
BlackBerry Proxy cluster	Select this option to specify the BlackBerry Proxy clusters that must be used to reach the domain.
Direct	Select this option to route traffic from the app to the server without going through BlackBerry Proxy. This option is supported only for apps developed with BlackBerry Dynamics SDK version 6.0 and later.
Deny	Select this option to block the app from connecting to the server. This option is supported for apps developed with BlackBerry Dynamics SDK version 6.0 and later.

BlackBerry Dynamics connectivity profile setting	Description
Primary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the primary route the app uses to connect to the server.
Secondary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the backup route the app uses to connect to the domain if the primary cluster is down.
IP address ranges	A list of IP address ranges that BlackBerry Dynamics apps can access when they make a connection request using an IP address rather than a hostname. To add a new IP address range to the list, click + and configure the settings for the settings. To remove an IP address range from the list, click × beside the range that you want to remove.
Range	Specify a range of IP addresses that BlackBerry Dynamics apps can access when they make a connection request using an IP address rather than a hostname. Address ranges must be entered with a lower and upper bound address (for example, 192.168.2.0-192.168.2.255) or in IPv4 CIDR notation (for example, 192.168.2.0/24). For example: • Example of discrete addresses: 192.168.2.0-192.168.2.255 • Example of an entire subnet: 192.168.2.0/24
BlackBerry Proxy cluster	Select this option to specify the BlackBerry Proxy clusters that must be used to reach the IP address range.
Direct	Select this option to route traffic directly from the app to the IP address range without going through BlackBerry Proxy. This option is supported only for apps developed with BlackBerry Dynamics SKD version 6.0 and later.
Deny	Select this option to block the app from connecting to the IP address range. This option is supported for apps developed with BlackBerry Dynamics SDK version 6.0 and later.
Primary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the primary route that the app uses to connect to the IP address range.
Secondary	Select the name of the BlackBerry Proxy cluster from the drop-down list to use as the backup route the app uses to connect to the IP address range if the primary cluster is down.
App servers	

BlackBerry Dynamics connectivity profile setting	Description
Add	If you have one or more BlackBerry Dynamics apps that are served from an app server or web server, you can specify the name and port of the server and the priority of the BlackBerry Proxy clusters used for communication with it. You can also set the priority of the app server to the client app as primary, secondary, or tertiary. All BlackBerry Dynamics apps served by the app server or web server are able to use the connection settings you specify. If you have BlackBerry UEM Cloud and a BEMS Cloud in your environment and you configured Email notifications or BEMS-Docs to create a BEMS tenant, the BEMS Cloud URL, port number, and priority are added automatically to the App servers payload section. For more information, see Add an app server to a BlackBerry Dynamics connectivity profile.

Export BlackBerry Dynamics connectivity profile settings

You can export BlackBerry Dynamics connectivity profile settings to a .csv file if you need to create additional profiles with similar settings.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Networks and connections > BlackBerry Dynamics connectivity**.
3. Click the name of the profile that you want to export.
4. Click ➔.
5. Click **Cancel** to close the profile without saving changes.

Add an app server to a BlackBerry Dynamics connectivity profile

If you have a BlackBerry Dynamics app that is served from an app server or web server, you can specify the name of that server and the priority of the BlackBerry Proxy clusters used for communication with it.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Networks and connections > BlackBerry Dynamics connectivity**.
3. Click the BlackBerry Dynamics connectivity profile that you want to add an app server to.
4. Click ✎.
5. Under **App servers**, click **Add**.
6. Select the BlackBerry Dynamics app that you want to add an app server for.
7. Click **Save**.
8. In the table for the app, click +.
9. In the **Server** field, specify the FQDN of the app server.
10. In the **Port** field, specify the listening port of the app server.
11. In the **Priority** drop-down list, specify the priority of the app or app entitlement. For example, if you have two BlackBerry Enterprise Mobility Server servers, and you prefer that all connections go to BEMS 1 first, you specify the BEMS 1 entry as the priority primary. You can then specify that BEMS 2 is always secondary.
12. Select a **Route type**.

13. In the **Primary** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
14. In the **Secondary** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
15. Click **Save**.

Controlling BlackBerry Dynamics on users devices

The BlackBerry Dynamics profile enables BlackBerry Dynamics for users and sets standards for BlackBerry Dynamics app access, data protection, and logging.

BlackBerry UEM includes a Default BlackBerry Dynamics profile with preconfigured settings. If no BlackBerry Dynamics profile is assigned to a user account or user group that a user belongs to, or a device group that a user's devices belong to, the default profile is sent to a user's devices.

UEM automatically sends a BlackBerry Dynamics profile to a device when a user activates it, when you update an assigned BlackBerry Dynamics connectivity profile, or when you assign a different BlackBerry Dynamics connectivity profile to a user account or device.

Create a BlackBerry Dynamics profile

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Policy > BlackBerry Dynamics**.
3. Click +.
4. Type a name and description for the profile.
5. Configure the appropriate values for the profile settings. For more information about each profile setting, see BlackBerry Dynamics profile settings.
6. Click **Add**.

After you finish: If necessary, rank the profile.

BlackBerry Dynamics profile settings

BlackBerry Dynamics profiles are supported on the following device types:

- iOS
- macOS
- Android
- Windows

BlackBerry Dynamics profile setting	Description
Configuration	
Require device management to use BlackBerry Dynamics apps	This setting specifies whether a device must be activated with MDM to use BlackBerry Dynamics apps.

BlackBerry Dynamics profile setting	Description
Enable UEM Client to enroll in BlackBerry Dynamics	If a device is using the BlackBerry UEM Client, this setting specifies whether BlackBerry Dynamics manages the activation of BlackBerry Dynamics apps and whether BlackBerry Dynamics apps can be used on the device. If this option is not selected, BlackBerry Dynamics apps could be removed from the device because the device will not be enabled for BlackBerry Dynamics. If you do not plan to use BlackBerry Dynamics in your environment, do not select this setting.
Enable BlackBerry Dynamics Launcher in UEM Client	This setting specifies whether the BlackBerry Dynamics Launcher icon appears in the UEM Client.
Enable BlackBerry Dynamics Launcher first time setup	When the BlackBerry Dynamics Launcher is enabled in the UEM Client and appears for the first time, this setting specifies whether the tutorial appears.
Start Entra Conditional Access enrollment after authentication broker is installed	If you configure Entra ID conditional access, you can enable this setting to delay the conditional access enrollment process until the Microsoft Authenticator app is installed on the device. This setting is turned off by default. If enabled, after the Microsoft Authenticator app is installed, the conditional access enrollment process is initiated when the user opens the UEM Client. On Android devices, if the work profile is unlocked, the UEM Client will prompt the user to open the UEM Client to start the conditional access enrollment. This option does not apply to Android devices with the User privacy activation type (it does apply to devices with Android Enterprise user privacy and Android Management user privacy). For User privacy devices, conditional access enrollment is always initiated after the device is activated with UEM.
Password	
Password expiration	This setting specifies whether the password for a BlackBerry Dynamics app expires and the number of days a password remains valid before it expires.
Do not allow previous passwords	This setting specifies whether previous passwords can be used and the maximum number of previous passwords that cannot be used for a BlackBerry Dynamics app.
Minimum password length	This setting specifies the minimum length of the password for a BlackBerry Dynamics app.
Allowed occurrences of a character	This setting specifies how many times a character can appear in a password for a BlackBerry Dynamics app.
Require both letters and numbers	This setting specifies whether the password must contain both letters and numbers for a BlackBerry Dynamics app.
Require both uppercase and lowercase	This setting specifies whether the password must contain both uppercase and lowercase letters for a BlackBerry Dynamics app.

BlackBerry Dynamics profile setting	Description
Require at least one special character	This setting specifies whether the password must contain at least one special character for a BlackBerry Dynamics app.
Do not allow sequences of more than two numbers	This setting specifies whether the password can contain more than two sequential numbers (for example,1, 2, 3) for a BlackBerry Dynamics app.
Do not allow more than one password change per day	This setting specifies whether a password can be changed more than once every 24 hours for a BlackBerry Dynamics app.
Do not allow personal information	This setting specifies whether the following personal information can be used in a password for a BlackBerry Dynamics app: • The user's first and last names (excluding initials) as recorded in Active Directory • The part of an email address before the @ sign.
Do not allow password entry if screen overlay detected on Android devices	This setting specifies whether a password can be entered in a BlackBerry Dynamics app when screen overlay is detected.
Allow Biometrics	This setting specifies whether BlackBerry Dynamics apps can be unlocked using biometric input when they are already open in the app switcher on iOS devices.
Enable Touch ID and Face ID when the device or app restarts	This setting specifies whether BlackBerry Dynamics apps can be unlocked using the selected biometric input methods when they are opened for the first time after a device restarts.
Require password to be re-entered and disable Touch ID and Face ID	This setting specifies a period of time after which users must enter a password to unlock a BlackBerry Dynamics app and re-enable Touch ID, Face ID, or both.
Permit fallback to device passcode if biometric authentication fails	This option allows iOS biometric (TouchID/FaceID) authentication to fall back to the device passcode if biometric authentication fails.
Allow Android biometric authentication	This setting specifies whether BlackBerry Dynamics apps can be unlocked using any device-supported biometric authentication method. If this option is not selected, all Android biometric authentication features are blocked, including fingerprint, iris, and face recognition.
Enable Android biometric authentication after the device or app restarts	This setting specifies whether BlackBerry Dynamics apps can be unlocked using biometric authentication when they are opened for the first time after a device restarts.

BlackBerry Dynamics profile setting	Description
Require password to be re-entered and disable Android biometric authentication	This setting specifies a period of time after which users must enter a password to unlock a BlackBerry Dynamics app and re-enable Android biometric authentication.
Do not require password	These settings specify whether a user can access a BlackBerry Dynamics app without entering a password.
iOS: Do not require authentication when securely receiving a file from an authenticated Dynamics app	This setting specifies whether iOS device users need to authenticate with a BlackBerry Dynamics app when they receive a secure file transfer from another BlackBerry Dynamics app that they have already authenticated with. By default, this setting is not enabled.
Blocked password list	
Blocked password file (.txt)	This setting specifies a list of banned passwords. You can download the previously uploaded list of banned passwords. Passwords in the list must meet the following requirements: each password must be separated by a hard return, only UTF-8 characters are supported, and passwords must be 14 characters or less.
Lock screen	
Require password when BlackBerry Dynamics apps start	This setting specifies whether a password is required each time a BlackBerry Dynamics app is started. If you are using authentication delegation, do not select this option.
Require password after period of inactivity	This setting specifies the period of inactivity that must elapse before a password is required.
Take action after invalid password attempts	This setting specifies whether there is a limit to the number of times that a user can enter an incorrect password. If you select this rule, specify the number of times that a user can enter an incorrect password and the action that occurs after the limit has been reached.
Wearables	
Allow WatchOS apps	This setting allows end users to pair their Apple WatchOS apps with the supported BlackBerry Dynamics apps on their iOS device.
Allow wearables	**Note:** This setting is deprecated in UEM version 12.19 and later. This setting specifies whether BlackBerry Dynamics apps can be used on an Android wearable device. If you select this rule, specify how much time must elapse before the wearable device is disconnected and whether the wearable can reconnect automatically.
App authentication delegation (iOS and Android only)	

BlackBerry Dynamics profile setting	Description
App	You can designate a BlackBerry Dynamics app to act as the authentication delegate on behalf of other other BlackBerry Dynamics apps so that users do not have to create a password for each BlackBerry Dynamics app that they install. After an authentication delegate is configured, each time a user opens a BlackBerry Dynamics app, the device displays the password screen for the authentication delegate instead of the app that they are attempting to open. After the user enters the password for the authentication delegate, the user can open the BlackBerry Dynamics app. You can choose any app to be the authentication delegate for other apps, but it is recommended that you choose your most commonly used app to be the primary authentication delegate to provide the most seamless experience for the user. As a best practice, it is recommended that you set only one authentication delegate. This prevents unnecessarily complex and undesirable authentication delegate switching and simplifies administrative management. If a user accidentally deletes the authentication delegate, they must reinstall it. If more than one authentication delegate is required, for example, the primary authentication delegate does not exist for a given platform and an alternate delegate is configured, refer to the following recommendations to make sure that BlackBerry Dynamics apps are successfully installed and activated: • Users should always install the primary authentication delegate first and they should not activate it using an already installed, alternate authentication delegate app. • If the user already has an alternate authentication delegate installed and in use, and then later installs the primary authentication delegate, they need to make sure that the existing, installed authentication delegate is in an unlocked state to successfully complete the authentication. If the alternate authentication delegate has been force closed, the user will encounter various errors and may be blocked. • Users must not delete the currently installed authentication delegate after they install their primary authentication delegate. Apps that are currently using that authentication delegate will need to automatically switch to the new authentication delegate when the app is next launched in online mode. • If the primary authentication delegate is deleted, users should reactivate the authentication delegate using an access key. If they attempt to activate the authentication delegate with any other app, it may cause various errors. • Even if the **Allow self-authentication when no authentication delegate application is detected** option is selected, or if an app that is designated as a secondary or tertiary authentication delegate is installed, there is no fallback mechanism to allow apps to change the authentication delegate without the original authentication delegate being installed and unlocked. • Select the **Allow self-authentication when no authentication delegate application is detect** option if you want to allow the user to authenticate the app when an authentication delegate is not installed on a device.

BlackBerry Dynamics profile setting	Description
Background activity (iOS and Android)	This setting enables background process restarts if the operating system has terminated the application process. When enabled, an app may use secure networking and storage in the background after receiving a push notification. This feature requires an Android version of the BlackBerry Dynamics apps set to be released in Fall 2025 or later.
Data leakage prevention	
Do not allow copying data from BlackBerry Dynamics apps into non-BlackBerry Dynamics apps	This setting specifies whether users can copy data from BlackBerry Dynamics apps into non-BlackBerry Dynamics apps.
Character limit for cut and copy	This setting specifies the character limit for copying and cutting in a BlackBerry Dynamics app. This feature requires a version of the BlackBerry Dynamics apps set to be released in Fall 2025 or later.
Do not allow copying data from non-BlackBerry Dynamics apps into BlackBerry Dynamics apps	This setting specifies whether users can copy data from non-BlackBerry Dynamics apps to BlackBerry Dynamics apps. **Note:** If you are using an app-based PKI solution such as Purebred, do not select this option.
Writing and AI tools	
Allow Apple Intelligence in-app writing tools	This setting specifies whether iOS users are able to access built-in Apple Intelligence writing tools within BlackBerry Dynamics apps. This setting is enforced only if the following data leakage prevention setting is enabled in the profile: "Do not allow copying data from BlackBerry Dynamics apps into non-BlackBerry Dynamics apps". If this DLP setting is not selected, Apple Intelligence writing tools are allowed in BlackBerry Dynamics apps. Note that if you turn off the IT policy rule "Allow writing tools (supervised only)" in the assigned IT policy, writing tools will be blocked for all apps on supervised iOS devices, regardless of the configuration of this setting in the BlackBerry Dynamics profile. By default, the "Allow writing tools (supervised only)" IT policy rule is enabled.
Screen capture and sharing	

BlackBerry Dynamics profile setting	Description
Do not allow screenshots (iOS)	This setting specifies whether users can take screenshots in BlackBerry Dynamics apps on iOS devices. If you enable this setting, when a device user tries to take a screenshot in a BlackBerry Dynamics app, a blank image with the following message is saved instead: "Your organization prevents screenshots being taken within this app." This option is supported for BlackBerry Dynamics apps that use BlackBerry Dynamics SDK 12.1 and later, and replaces the iOS screen capture detection rule in compliance profiles. BlackBerry recommends using this profile setting and disabling the iOS screen capture compliance rule. The compliance rule will be deprecated in a future UEM release.
Do not allow screen recording and sharing on iOS devices	This setting specifies whether an iOS user can use screen sharing or recording in a BlackBerry Dynamics app.
Do not allow screen capture and insecure video output (Android)	This setting specifies whether Android device users can take screen captures and record insecure video in BlackBerry Dynamics apps.
Dictation and custom keyboards	
Do not allow dictation (iOS and Android)	This setting specifies whether users can use voice dictation with BlackBerry Dynamics apps. This setting applies to application-specific uses of voice dictation and might not apply to the keyboard, which can allow dictation through other channels.
Do not allow custom keyboards (iOS and Android)	This setting specifies whether iOS or Android users can use custom keyboards in BlackBerry Dynamics apps.
Enable Android keyboard restricted mode	This setting specifies whether personalized learning is disabled on Android keyboards. This setting is only applicable to keyboards that support turning off the personalized learning feature.
Transfer files	
Open files unencrypted in other selected non-Dynamics apps	This setting specifies whether users are allowed to share files to a list of non-BlackBerry Dynamics apps. This feature requires a version of the BlackBerry Dynamics apps set to be released in Fall 2025 or later.
Open in selected apps	This setting specifies which non-BlackBerry Dynamics apps are allowed to open files shared from BlackBerry Dynamics apps. This feature requires a version of the BlackBerry Dynamics apps set to be released in Fall 2025 or later.
Encryption of data	

BlackBerry Dynamics profile setting	Description
Enable FIPS	This setting specifies whether compliance with U.S. Federal Information Processing standard 140-2 is enforced. Federal Information Processing Standards (FIPS) are U.S. government regulations regarding computing and computing security. When you enable FIPS compliance, the major effect is on associated applications. Enabling FIPS compliance enforces the following constraints in conformance with FIPS: • MD4 and MD5 are prohibited by FIPS, which means that access to NTLM- or NTLM2-protected web pages and files is blocked. • Wrapped applications are blocked. • In secure socket key exchanges with ephemeral keys, with servers that are not configured to use Diffie-Hellman keys of sufficient length, BlackBerry Dynamics retries with static RSA cipher suites.
Certificates	
Trusted Certificate Authorities	This setting specifies whether BlackBerry Dynamics apps can get certificates from the device certificate store.
Detailed logging	
Enable detailed logging for BlackBerry Dynamics apps	This setting specifies whether log files can be generated and uploaded from BlackBerry Dynamics apps.
Prevent users from turning on detailed logging in BlackBerry Dynamics apps	This setting specifies whether users can turn on the ability to generate and share detailed log files from BlackBerry Dynamics apps.
Agreement	
Enable an agreement message for BlackBerry Dynamics apps	This setting specifies whether to display a message in BlackBerry Dynamics apps that the user must acknowledge. If authentication delegation is enabled, the message is displayed only in the authenticator app. If you select this rule, complete the following actions: • Specify if the message is displayed each time the app is unlocked, otherwise the message is only displayed the first time the user opens the app. • In the **Message** field, create the message that you want to display. On Android devices, only the first 4000 characters are displayed.

Send device commands to BlackBerry Dynamics apps in UEM

If any BlackBerry Dynamics app has been installed on a device, you can perform actions on the app. For example, you can delete app data if a user has lost a device.

1. In the management console, on the menu bar, click **Users**.
2. Search for a user account.
3. In the search results, click the name of the user account.

4. Select the device tab for the device that has installed the app that you want to manage.
5. Expand the **BlackBerry Dynamics apps** section.
6. Locate the row for the BlackBerry Dynamics app to send a device command to.
7. Click the three dots in the **App actions** column to perform one of the following actions:

Task	Description
Lock app.	Lock the BlackBerry Dynamics app. This is useful when a user has lost a device but may recover it. The app cannot be accessed but app data is not deleted.
Unlock app.	Unlock the BlackBerry Dynamics app. The user regains access to the app and app data.
Delete app data.	Delete all data for the BlackBerry Dynamics app and make the app unusable. The app data cannot be recovered. This is useful when a user has lost a device and cannot recover it.
Logging on.	Turn on app logging. Logging is set to debug level.
Logging off.	Turn off app logging.
Upload log files.	Upload the app logs from the device to the BlackBerry Dynamics NOC.
Get app events.	Display detailed information about compliance and other app events.
App details	Displays detailed information about the app including the Container ID.

Manage settings for a BlackBerry Dynamics app

You can manage app configurations, server configurations, and app settings.

1. In the management console, on the menu bar, click **Apps**.
2. Click the BlackBerry Dynamics app that you want to change.
3. On the **Settings > BlackBerry Dynamics** tab, perform any of the following tasks:

Task	Steps
Specify a BlackBerry Dynamics profile for the app.	If you want the app to use a specific BlackBerry Dynamics profile instead of the BlackBerry Dynamics profile that is assigned to the user, select the profile from the **Override BlackBerry Dynamics profile** drop-down list.
Specify a compliance profile for the app.	If you want the app to use a specific compliance profile rather than the compliance profile that is assigned to the user, select the profile from the **Override compliance profile** drop-down list.
Specify a BlackBerry Dynamics connectivity profile for the app.	If you want the app to use a specific BlackBerry Dynamics connectivity profile instead of the BlackBerry Dynamics connectivity profile that is assigned to the user, select the profile from the **Override BlackBerry Dynamics connectivity profile** drop-down list.

Task	Steps
Add or change the app configuration for an internal app.	**a.** Beside **App configuration**, click **Upload a template** to add a new app configuration template. **b.** Browse to the location of the template. **c.** Click **Save**. For more information on creating the template, see the BlackBerry Dynamics SDK Development Guide.
Add, copy, or change the app configuration for a public app.	**a.** In the **App configuration** table, click +. Do one of the following: **1.** To create a new configuration, click **Create new**. Enter a name and edit the configuration settings. **2.** To copy from an existing app configuration, click **Copy from an app configuration**. Enter a name, select an existing app configuration from the drop-down list and edit the configuration settings. **b.** Click **Save**. **c.** If required, use the arrows to move the app configuration up or down to change the ranking. For more information see BlackBerry UEM Client app configuration settings. For more information about BlackBerry Work, BlackBerry Notes and BlackBerry Tasks app configuration settings, see Configure BlackBerry Work app settings and Configure BlackBerry Notes and BlackBerry Tasks app settings in the BlackBerry Work, Notes, and Tasks Administration content.
Add or change the server configuration payload to specify the keys and values used to configure settings for the app.	If the app has custom app policies, the custom policies are added to the Server configuration payload area. **a.** In the **Server configuration payload** section, click **Add**. **b.** In the text box, enter the XML or JSON code for the configuration payload.
Allow BlackBerry Dynamics apps to use user certificates, SCEP profiles, and user credential profiles.	Select whether the app can use user certificates as an authentication option. For more information about configuring your environment to using certificates with BlackBerry Dynamics apps, see Sending certificates to devices and apps using profiles.

4. Click the tab for the device platform that you want to manage and set the appropriate options.
5. Click **Save**.

iOS and macOS: BlackBerry Dynamics app settings

Most of the following settings are supported only for iOS devices and don't appear on the macOS tab.

iOS and macOS settings	Description
iOS or macOS Bundle ID	This setting specifies the package ID for the app.
App name	This setting specifies the name of the app that appears on the app list.

iOS and macOS settings	Description
Vendor	This setting specifies the vendor of the app.
App description	This setting specifies the app description.
Category	This setting specifies a category 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 or type a name to create a new category.
Screenshots	This setting specifies screenshots for the app. Click "Add" to select the images. The supported image types are .jpg, .jpeg, .png, or .gif.
Supported device form factor	This setting specifies 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 on iPad devices.
Remove the app from the device when the device is removed from BlackBerry UEM	This setting specifies whether the app is deleted from the device when the device is removed from UEM. This setting applies only to apps with a disposition marked as "Required" and the default installation for required apps is set to "Prompt once."
Disable iCloud backup for the app	This setting specifies whether the app can be backed up to the iCloud online service. This option applies only to apps with a disposition marked as "Required."
Default installation for required apps	This setting specifies whether users are prompted to install required apps. Select one of the following options: • **Prompt once**: users to receive one prompt to install the app on their iOS devices. 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. • **No prompt**: Users don't receive a prompt to install the app. This setting applies only to apps with the disposition set to "Required." You set the disposition of the app when you assign the app to a user or group.
Convert installed personal app to work app	This setting specifies whether to convert the app to a work app if it is already installed on iOS devices. If you 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.
Restricted versions	This setting specifies versions of the app that you want to prevent users from installing on their devices. If you add multiple versions, separate each version with a comma.

Android: BlackBerry Dynamics app settings

Android settings	Description
Add internal app source file	This setting specifies the location of the internal app source file for the public store app. To add internal app source files, see Upload BlackBerry Dynamics app source files.
Android package name	This setting specifies the package ID for the app.
App name	This setting specifies the name of the app that appears on the app list.
Vendor	This setting specifies the vendor of the app.
App description	This setting specifies the app description.
Category	This setting specifies a category 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 or type a name to create a new category.
Send to	This setting specifies whether the app is sent to all Android devices, only Android Enterprise devices, or only Samsung Knox Workspace devices.
Restricted versions	This setting specifies versions of the app that you want to prevent users from installing on their devices. If you add multiple versions, separate each version with a comma.

Windows: BlackBerry Dynamics app settings

Windows settings	Description
Windows 10 (UWP) app package ID	This setting specifies the package family name for a Windows 10 app.
App name	This setting specifies the name of the app that appears on the app list.
Vendor	This setting specifies the vendor of the app.
App description	This setting specifies the app description.
Category	This setting specifies a category 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 or type a name to create a new category.
Screenshots	This setting specifies screenshots for the app. Click "Add" to select the images. The supported image types are .jpg, .jpeg, .png, or .gif.

Windows settings	Description
Remove the app from the device when the device is removed from BlackBerry UEM	This setting specifies whether the app is deleted from the device when the device is removed from BlackBerry UEM. This setting applies only to apps with a disposition marked as "Required" and the default installation for required apps is set to "Prompt once."
Restricted versions	This setting specifies versions of the app that you want to prevent users from installing on their devices. If you add multiple versions, separate each version with a comma.

BlackBerry UEM Client app configuration settings

Option	Description
Enable Bypass Unlock	If you select this option, the UEM Client will bypass the BlackBerry Dynamics user authentication/lock screen and the user can open the UEM Client without needing to unlock the UEM Client app. If you have BlackBerry 2FA configured, the BlackBerry 2FA accept/decline screen will display and the user must accept. Then user is then logged in to the app or service through BlackBerry 2FA.
App name	Type a name for the app. You select this option when you want to use your organization's app-based PKI solution, such as Purebred, to enroll certificates for BlackBerry Dynamics apps. You can install the app on devices and allow BlackBerry Dynamics apps to use certificates enrolled through the PKI app. This option is supported only for iOS devices
UTI schemes	Specify the UTI schemes for your organization's app-based PKI solution. If you are using the Purebred app, use one of the following schemes: • Purebred Registration 2025 app: `purebred2025.select.all-user`, `purebred2025.select.no-filter`, `purebred2025.zip.all-user`, `purebred2025.zip.no-filter` • Pre-2025 Purebred app: `purebred.select.all-user`, `purebred.select.no-filter`, `purebred.zip.all-user`, `purebred.zip.no-filter` Note that the UTI schemes for the Purebred 2025 app take precedence over the UTI schemes for the pre-2025 Purebred app. It is recommended to not use both sets of Purebred UTI schemes, and to not have both the 2025 and pre-2025 Purebred apps on the same device, as it can cause issues when importing Purebred certificates into the UEM Client. If you are using the pre-2025 Purebred app, you must turn off the following rule in the IT policy assigned to users: “Do not allow copying data from non BlackBerry Dynamics apps into BlackBerry Dynamics apps”.

Configure a third-party identity provider for activating BlackBerry Dynamics apps on a device

You can configure a third-party identity provider so that users can sign-in with their directory credentials to activate BlackBerry Dynamics apps on a device. They can also use it to unlock an app or reset their BlackBerry Dynamics app password.

Before you begin: To configure this feature, you need the following:

- BlackBerry Dynamics apps compiled with a supported version of the BlackBerry Dynamics SDK.
- BlackBerry Enterprise Identity is enabled.

1. Configure your organization's third-party identity provider to work with BlackBerry Enterprise Identity.
    - For information about configuring Okta and BlackBerry Enterprise Identity, see the BlackBerry Enterprise Identity Administration Guide. Ensure that the Microsoft Active Directory that your organization's Okta instance uses is also configured in BlackBerry UEM through **Settings > External Integration > Company Directory**.
    - For information about configuring PingFederate and BlackBerry Enterprise Identity, see the BlackBerry Enterprise Identity Administration Guide.
2. Do one of the following:
    - If you are using PingFederate or Okta, enable **Dynamics Activation via Enterprise IDP** as an OpenID Connect app.
    - If you are using Active Directory as the identity provider, add the **Dynamics Active Directory Activation** as an OpenID Connect app.

    For more information, see the BlackBerry Enterprise Identity Administration Guide.
3. In BlackBerry UEM, set up your organization's identity provider. For more information, see the BlackBerry Enterprise Identity Administration Guide PingFederate and Okta instructions.
4. In BlackBerry UEM, create a BlackBerry Enterprise Identity Authentication policy. Ensure you select **Manage service exceptions**, and add the **Dynamics Activation via Enterprise IDP** service. For more information, see the BlackBerry Enterprise Identity Administration Guide.
5. Assign the BlackBerry Enterprise Identity Authentication policy to users. For more information, see the BlackBerry Enterprise Identity Administration Guide.

After you finish:

- During the activation process, users need to select the **Sign in with your organization if instructed by your administrator** option and sign in using your organization's identity provider.
- For more information, .

Automatically activate the first BlackBerry Dynamics app on Apple DEP and User Enrollment devices

During the activation of Apple DEP devices or iOS devices using the User privacy - User enrollment activation type, the BlackBerry Dynamics app that is the primary authentication delegate can be installed first and preconfigured so that when the user opens it for the first time, it automatically activates without requiring the user to manually enter information. Users can use this app to easily activate other BlackBerry Dynamics apps on their devices.

To automatically activate the first BlackBerry Dynamics app on an iOS device:

1. Make sure that the device that you want to activate is registered with Apple DEP or assigned the User privacy - User enrollment activation type.
2. In the BlackBerry Dynamics profile, set a BlackBerry Dynamics app as the primary authentication delegate. For example, if BlackBerry Work is the most frequently used app, set it as the primary authentication delegate.

   Note: For iOS devices enrolled in DEP, do not set BlackBerry UEM Client as the primary authentication delegate.
3. Assign the app that's the primary authentication delegate to the user with a Required disposition.

Manage BlackBerry Dynamics app services

App services are shared functions that are offered by a mobile or server-based app. Using the BlackBerry Dynamics SDKs, an app developer can expose a function of an app that other developers can use in their own BlackBerry Dynamics apps. Using the management console, you can register app services for your organization and supply the service definition from the developer. Your organization's developers can review the registered app services and can leverage the available service definitions in the BlackBerry Dynamics apps that they create.

App services for select BlackBerry Dynamics apps and partner apps are also available for use, and you can view the associated service definitions in the management console. For more information about app service development, visit the BlackBerry Developer Community.

Before you begin: If you want to register an app service for your organization, verify that you have the app service ID, version number, and service definition.

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **App services**.
3. Perform any of the following tasks:

Task	Steps
Register an app service for your organization.	**a.** Click +. **b.** In the **Service type** drop-down list, perform one of the following actions: • If the app service is offered by a mobile app, click **Application**. • If the app service is offered by a server-based app, click **Server**. **c.** In the **ID** field, type the app service ID. The ID must be a unique string (all lowercase) in reverse DNS notation (for example, com.example.service.print). **d.** Type a name and description for the app service. **e.** In the **Version** field, type the version. The version number must include digits only. If you want to add one or more sub-version numbers (for example, the build version), use periods to separate the segments. Each segment cannot begin with 0 (for example, 1.1.5 is valid, 1.1.05 is not). **f.** Optionally, type a description for the version. **g.** In the **Service definition** field, type the service definition in JSON format. **h.** Click **Save**.

Task	Steps
Edit an app service.	Use the following steps to edit an app service that was registered for your organization (for example, to add a new version). You cannot change the app service type or ID. You cannot edit a BlackBerry Dynamics app service or partner app service. **a.** Search for the app service that you want to edit. **b.** Click the app service name. **c.** Edit the app service details as necessary. **Note:** Deleting an app service version does not have any impact on the apps that offer or use the service, it simply removes the service definition from the management console so that your organization's developers cannot refer to it. **d.** Click **Save**.
Delete an app service.	You cannot delete a BlackBerry Dynamics app service or partner app service. Deleting an app service from the management console does not have any impact on the apps that offer or use the service, it simply removes the service definition from the management console so that your organization's developers cannot refer to it. **a.** Search for the app service that you want to remove. **b.** Click ✕ next to the service. **c.** Click **Delete**.

After you finish: Optionally, you can bind an app service version to a managed app so that the management console can indicate that the app provides the service. For more information, see Manage settings for a BlackBerry Dynamics app.

Rank app installations

You can rank apps to control the order that the apps are installed when you assign them to devices. Setting the rank ensures that any BlackBerry Dynamics authentication delegate apps are pushed to the device first. For iOS apps, the ranking applies to public apps and apps hosted in BlackBerry UEM. For Android apps, the ranking applies to apps hosted in BlackBerry UEM or Google Play.

The ranking of apps hosted in Google Play is supported only on devices that are activated with Android Enterprise and enabled for Google Play. The ranking of apps hosted in BlackBerry UEM and apps hosted in Google Play are applied separately. To enable a device for Google Play, select one of the following options when you create the activation profile:

- Add Google Play account to work space
- Google Play app management for Samsung Knox Workspace devices

1. In the management console, on the menu bar click, **Apps > App installation ranking**.
2. Click ✎.
3. Do any of the following:
    - To add the apps that you want to rank, click +, select the apps, and click **Add**.
    - To remove an app from ranking, click ✕ beside the app that you want to remove and click **Remove**.

4. In the **Rank** column, click ↓↑ to place the apps in the order that you want them to be installed on the devices.
5. Click **Save**.

Add the work app catalog to the BlackBerry Dynamics Launcher

For devices that are enabled for BlackBerry Dynamics, you can add the work app catalog to the BlackBerry Dynamics Launcher so that users have quick access to a list of their assigned work apps.

Note: BlackBerry Access must be installed and active on a device for the work app catalog to appear in BlackBerry Dynamics Launcher.

1. In the management console, on the menu bar, click **Groups**.
2. Select the **All users** group.
3. In the **Assigned apps** section, click +.
4. In the search field, search for **Feature – BlackBerry App Store**.
5. Select **Feature – BlackBerry App Store**.
6. In the **Disposition** drop-down list for the app, select **Required**.
7. Click **Assign**.

Generate access keys, activation passwords, or QR codes for BlackBerry Dynamics apps

BlackBerry Dynamics apps require an access key, activation passwords, or QR codes to be activated on a device. The BlackBerry UEM Client can request access keys or activation passwords automatically from BlackBerry UEM after users install an app. You or a user must manually generate access keys, activation passwords, or QR codes and send them to activate BlackBerry Dynamics apps in the following scenarios:

- For Samsung Knox Workspace devices
- For iOS and Android devices that don't need MDM and do not have the UEM Client installed
- For users who want to activate BlackBerry Dynamics apps on devices that don't require the UEM Client

You can generate access keys, activation passwords, or QR codes when you create a new user, or anytime afterwards. Users do not need to activate their devices on UEM to receive access keys, activation passwords, or QR codes. Users do not require an email address for you to generate an access key, activation password, or QR code. Users can also generate access keys, activation passwords, or QR codes in BlackBerry UEM Self-Service (users cannot specify the expiry period).

1. In the management console, on the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Click **Set activation password**. Complete one of the following tasks:

Tasks	Steps
Generate an activation password and QR code. This feature requires that the BlackBerry Dynamics app is running a software version that includes BlackBerry Dynamics SDK 8.0 or later.	**a.** In the **Activation option** drop-down list, select **Device activation with specified activation profile**. **b.** In the **Activation profile** drop-down list, select the activation profile that you want the password to be paired with. **c.** In the **Activation password** drop-down list, perform one of the following tasks: • If you want to automatically generate a password, select **Autogenerate device activation password and send email with activation instructions**. When you select this option, you must select an email template to send the information to the user. • If you want to set an activation password for the user and, optionally, send an activation email, select **Set device activation password**. **d.** Optionally, change the activation period expiration. The activation period expiration specifies how long the activation password remains valid. **e.** In the **Activation email template** drop-down list, select the email template that you want to use. **f.** Click **Submit**. If the user does not have an email address, to find the activation password and QR code, click the **View activation email** link in the **Activation details** section, under **Device activation password**.
Generate an access key.	**a.** In the **Activation option** drop-down list, select **BlackBerry Dynamics access key generation**. **b.** In the **Number of access keys to generate** drop-down list, select the number of access keys that you want to create for the user. **c.** Select the number of days that you want the access keys to remain valid. **d.** In the **Email template** drop-down list, select the email template that you want to use. If the user does not have an email address, select **None**. **e.** Click **Submit**. If the user does not have an email address, to find the access key, click the link that displays the number of generated keys in the **Activation details** section, under **BlackBerry Dynamics access keys**.

After you finish: In the **Activation details** section of the user account screen, you can click the number beside **BlackBerry Dynamics access keys** to see a list of generated access keys. You can resend (✉) or delete (✕) the keys that were generated.

Send a BlackBerry Dynamics app unlock key and QR code to a user

You can send an email with an app unlock key and QR code to a user if a BlackBerry Dynamics apps has become locked on their device. The user can also generate an unlock key for a BlackBerry Dynamics app using UEM Self-

Service. For BlackBerry UEM version 12.21 Quick Fix 1 (February 2025) and later releases, the unlock key can be used for any BlackBerry Dynamics app on the device. The key expires after it is used to unlock a BlackBerry Dynamics app. You or the user must generate a new key for each app that the user wants to unlock.

1. In the management console, on the menu bar, click **Users**.
2. Search for and click the name of user account.
3. Click the appropriate device tab.
4. In the **BlackBerry Dynamics apps** section, in the **App actions** row, click **Unlock app** for a BlackBerry Dynamics app.
5. Select the BlackBerry Dynamics unlock key email template that you want to use.
6. Click **Send**.

Set up a screen capture rule for BlackBerry Dynamics apps on iOS devices

You can enable an option in a compliance policy that reacts to screen captures of BlackBerry Dynamics apps on iOS devices.

1. In the management console, on the menu bar, click **Policies and profiles**.
2. Click **Compliance > Compliance**.
3. Click **+**.
4. Type a name and description for the compliance profile.
5. Click the **iOS** tab.
6. Select **BlackBerry Dynamics screen capture detection on iOS devices**.
7. In the **Maximum number of screen captures within period** list, select a number.
8. In the **Period length** field, type a number of days that a session can last.
9. In the **Enforcement action for BlackBerry Dynamics apps** list, select the action that occurs if the user exceeds the allowed number of screen captures. Do one of the following:
    - Select **Monitor and log**: When a user takes a screen capture a warning message displays on the device that screen captures are prohibited.
    - Select **Do not allow BlackBerry Dynamics apps to run**: A message displays on the device that informs the user how long they are prevented from taking screen captures. If you make this selection, in the Allow all to run after field, type a number of minutes, hours, or days that you want the enforcement action to last.
10. Click **Save**.

Turn off notifications outside of work hours from BlackBerry Work

You can use Do not disturb profiles to block device notifications outside of work hours in BlackBerry Work for Android and BlackBerry Work for iOS.

Before you begin:

- BEMS is installed and configured in your environment. For instructions, see the BEMS installation and configuration guides.
- BlackBerry Work is added to the BlackBerry Dynamics connectivity profile. See Configure BlackBerry Work connection settings in the BlackBerry Work administration content.

1. In the management console, on the menu bar, click **Policies and profiles**.

2. Click **Protection > Do not disturb**.
3. Click +.
4. Type a name and description for the profile.
5. Enter a message to display on devices when BlackBerry Work notifications are blocked . If you leave this field blank, a default message is displayed.
6. Do one of the following:

Task	Steps
Specify common work days and hours.	a. Click the **Select common work days and hours** option. b. In the **From** drop-down lists, specify the time that work days start. c. In the **To** drop-down lists, specify the time that work days end. d. In the **Work days** list, select the days of the week that are work days.
Specify custom work hours for specific days.	a. Click the **Select custom work days and hours** option. b. Select a day of the week. c. In the **From** drop-down lists, specify the time that the work day starts. d. In the **To** drop-down lists, specify the time that the work day ends. e. Repeat steps 2 to 4 for each day of the week that is a work day.

7. Click **Add**.

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.

Intune uses app protection policies to protect apps and data. You can connect UEM to Intune to manage the app protection policies from the UEM management console using the Intune app protection profile for iOS and Android devices. When you create or update an app protection profile in UEM, the settings are sent to Intune where it updates the corresponding app protection policy.

To connect UEM to Intune so that you can deploy apps protected by Intune and manage the app protection profiles, see Configuring BlackBerry UEM to manage Microsoft Intune app protection profiles in the UEM Configuration content.

Note: Microsoft national cloud deployments do not support the APIs needed to connect UEM with Intune. UEM cannot integrate with Intune in national cloud deployments. For more information, see the Microsoft Graph documentation.

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 to directory-linked groups only.

After you create an app protection profile in UEM, you must update the profile in UEM and not the corresponding app protection policy in Intune. If you update the corresponding policy in Intune, the changes are not synchronized with the profile in UEM.

Before you begin:

- Configure the connection between UEM and Microsoft Intune. See Configuring BlackBerry UEM to manage Microsoft Intune app protection profiles in the Configuration content.
- For Android devices, ensure the Microsoft Company Portal app is installed on devices. For more information, see the Microsoft Intune documentation.

1. In the management console, 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. See the following:
    - Common: Microsoft Intune app protection profile settings
    - iOS: Microsoft Intune app protection profile settings
    - Android: Microsoft Intune app protection profile settings
6. Click **Add**.

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

Common: Microsoft Intune app protection profile settings

These settings correspond to Intune app protection policy settings. If you want more information about a setting, see the Microsoft Intune documentation.

Intune app protection profile setting	Description
Interoperability	
Enable interoperability between Intune and Dynamics apps	This setting specifies whether BlackBerry Dynamics apps can interact with Intune-managed apps, such as Microsoft 365 apps, on the device. To allow interoperability between BlackBerry Dynamics apps and Intune-managed apps, BlackBerry BRIDGE must be installed on users' devices. For more information, see the BlackBerry BRIDGE Administration Guide.
Custom JSON	Edit the JSON values to customize messages and warnings seen by your users in the BlackBerry BRIDGE app.
Data relocation	
Allow app to transfer data to other apps	This setting specifies the apps Intune-managed apps can send data to. The "Policy managed apps" option allows data to be transferred only to other apps that are managed by Intune. If the "Enable interoperability between Intune and Dynamics apps" setting is selected, you can't change this setting from the default option.
Allow app to receive data from other apps	This setting specifies the apps that apps managed by the app protection policy can receive data from. The "Policy managed apps" option allows data to be transferred only from other apps that are managed by Intune. If the "Enable interoperability between Intune and Dynamics apps" setting is selected, you can't change this setting from the default option.
Prevent "Save as"	This setting specifies whether the "Save As" option is enabled for apps. If you select this setting in an on-premises environment, you can allow using the "Save As" option to save work data only to one or more of the following locations: • Local storage • OneDrive for Business • SharePoint
Restrict cut, copy, and paste with other apps	This setting specifies how cut, copy, and paste operations can be used with the app. • 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.

Intune app protection profile setting	Description
Disable contact sync	This setting specifies whether the app can save contacts to the native Contacts app on the device.
Disable printing	This setting specifies whether the app can print data.
Inclusion group	This setting specifies whether the policy is deployed to inclusion groups.
Access	
Require corporate credentials for access	This setting specifies whether users must use their organization credentials to access the app. If this rule is selected, it takes precedence over requirements for a PIN or fingerprint.
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	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. If the "Require corporate credentials for access" setting is selected, it takes precedence over this rule.
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.

Intune app protection profile setting	Description
Disable app PIN when device PIN is managed	This setting specifies whether the app prompts for the PIN when the device is required to have a password. 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.
PIN character set	This setting specifies the types of characters the PIN must contain. • Numeric: The PIN must contain only numbers. • Alphanumeric and symbols: The PIN must contain letters, numbers, and symbols.
PIN reset	This setting specifies the number of days before the user must reset their PIN. The default setting is 90 days.

iOS: Microsoft Intune app protection profile settings

These settings correspond to Intune app protection policy settings. If you want more information about a setting, see the Microsoft Intune documentation.

Intune app protection profile setting	Description
Encrypt app data	This setting specifies when app data is encrypted. • 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 backups	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.

Intune app protection profile setting	Description
Restrict web content transfer with other apps	This setting specifies which browser opens web links in apps. • Any app: The user can choose which app opens the web link. • Intune Managed Browser: Web links can open in any browser managed by Intune. • Microsoft Edge: Web links open in Microsoft Edge. • BlackBerry Access: Web links open in BlackBerry Access. • Unmanaged browser: Web links can open in any browser not managed by Intune. You must specify the protocol used to open web links.
Unmanaged browser protocol	Specify the browser protocol that must be used to open web links, for example http or https. Web links can open in any browser that supports the protocol.
Require minimum iOS version	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 version (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	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). 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.
Require minimum app version (Warning only)	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). 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.
Minimum SDK version	This setting specifies the minimum Intune SDK version that is required from an app. If the SDK version does not meet the requirement, the user is blocked from accessing the app.
Face ID instead of PIN for access	This setting specifies whether the user is allowed to use Face ID to access the app instead of using their PIN.

Android: Microsoft Intune app protection profile settings

These settings correspond to Intune app protection policy settings. If you want more information about a setting, see the Microsoft Intune documentation.

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.
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.
Restrict web content transfer with other apps	This setting specifies which browser opens web links in apps. • Any app: The user can choose which app opens the web link. • Intune Managed Browser: Web links can open in any browser managed by Intune. • Microsoft Edge: Web links open in Microsoft Edge. • BlackBerry Access: Web links open in BlackBerry Access. • Unmanaged browser: Specify a browser not managed by Intune that opens web links.
Unmanaged Browser ID	Specify the app package ID for the browser that opens web links.
Unmanaged Browser Name	Enter the name of the app associated with the app package ID. If the user doesn't have the app installed, this name appears in the notification informing users to install the app.
Require minimum Android version	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. You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).
Require minimum Android version (Warning only)	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. You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).
Require minimum Android patch version	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. Specify the version using the date format YYYY-MM-DD.

Intune app protection profile setting	Description
Require minimum Android patch version (Warning only)	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. Specify the version using the date format YYYY-MM-DD.
Require minimum app version	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 up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2). 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.
Require minimum app version (Warning only)	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 up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2). 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.
Disable app encryption	This setting specifies whether app encryption is disabled if device encryption is enabled.

Wipe data for 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. In the management console, 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, including B2B 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

1. In the management console, 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.
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**.

After you finish:

- You can click ✏ to edit the VPP account name, account holder information, service token, and the automatic update settings.
- If you want to delete a Apple VPP account, you must remove apps that have associated licences from users before deleting it.

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 you assign apps to any of the following:

- User accounts
- App groups
- User groups
- Device groups

You can choose to have users install iOS VPP apps as personal apps that are not managed by UEM. You cannot use UEM to remove them from devices and the apps are not subject to UEM controls such as IT policy rules. When you assign an iOS VPP app to a user or group, set “Disposition” to Optional and the “Target” to Personal to redirect the user to the App Store to install the app as unmanaged. When you set the Disposition to Optional and the Target as Personal, you are prompted to assign the appropriate VPP license to devices so the app can be treated as unmanaged.

View Apple VPP license assignment

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

1. In the management console, 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
   - Whether the app license is assigned to a user account or a device
   - Whether a VPP license is used or not used
   - Whether the app is installed or not installed
4. Click **Close**.

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. In the compliance profile, you can also select an option to prevent apps from 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.
- For Android Enterprise devices, you only need to create compliance profile with enforcement actions if you want to restrict system apps (such as calculator, clock, or camera), because users can only install apps that you have assigned in the work space. 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 hidden 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

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 Enforcing compliance rules for devices.

Steps to prevent users from installing specific apps

When you prevent users from installing apps, you perform the following actions. Note that 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.

Step	Action
1	Add an app to the restricted app list. **Note:** This step does not apply to built-in apps for supervised iOS devices. To restrict built-in apps for supervised iOS devices, add the apps to the restricted app list in the compliance profile. For more information, see iOS: Compliance profile settings.
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 list of apps that you can select from when you want to enforce one of the following rules in the compliance profile:

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

Note: The following steps do not apply to built-in apps for supervised iOS devices. To restrict built-in apps for supervised iOS devices, you only need add the apps to the restricted app list in the compliance profile. For more information, see iOS : Compliance profile settings.

1. In the management console, 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.	**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.	**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.

After you finish: Create a compliance profile and assign it to users, user groups, or device groups.

Limit the apps that can run on a device

You can limit the use of a device to a single app or a set of apps using an app lock mode profile. For example, you can use an app lock mode profile to limit devices to run only one app for training purposes or for point-of-sales demonstrations. On iOS devices, the home button is disabled and the app automatically opens when the user reboots the device or wakes it.

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: You need the app package ID of the app, or if you plan to use the app list to select an app, make sure that the app is available in the app list.

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

Task	Steps
Specify the app to run on supervised iOS devices.	In the **Specify the app to run on the device** section, perform one of the following actions: • Click **Select an app from the app list**, click **Add an app**, and click an app in the list. • Click **Specify the app package ID of an app** and type the app package ID (for example, <*com.company.appname*>). 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 apps to run on Android devices (Android Enterprise and devices managed using Samsung Knox MDM).	Click + and do the following to specify the apps that you want to limit the device to: • Click **Specify the app package ID of an app** and type the app package ID (for example, <*com.company.appname*>) and the name of the app. Valid characters are uppercase and lowercase letters, 0 to 9, hyphen (-), and period (.). Click **Add**. • Click **Select an app from the app list**, and click an app in the list. Click **Add**. For Android Enterprise devices, if you want to limit the device to a specific app, click **Limit device to a single app** and select the app. The app that you specify in this setting automatically opens when the device starts and the user always returns to it. The app can access the other apps that you specify in the profile when it is required.

Task	Steps
Specify the app to run on Windows devices.	• 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 `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`.

6. 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.
7. For iOS devices, in the **User-enabled settings**, select the options that the user can enable.
8. Click **Add**.

After you finish: If necessary, rank the profiles.

View the list of personal apps in the management console

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.

This feature is not supported on devices that are activated with the following activation types:

- iOS and Android: User privacy
- Android 11 and later: Work and personal - full control (Android Enterprise fully managed device with work profile)
- Android: Work and personal - user privacy
- Samsung Knox: Work and personal - user privacy (Samsung Knox)
- iOS and Android: Device registration for BlackBerry 2FA only

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. In the management console, on the menu bar, click **Apps > Personal apps**.
2. To export the list of personal apps and related information to a .csv file, click ➜.
3. 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.
4. 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. In the management console, 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**.

After you finish: Assign the profile to users, user groups, or device groups.

Rating and reviewing apps

You can specify whether users in your organization can rate and review iOS, Android, and Windows 10 apps and allow them to see reviews provided by other users. Ratings and reviews submitted for apps cannot be seen by users outside your environment.

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 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 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 UEM.

Rating and reviewing apps is not supported on 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. In the management console, 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. In the management console, 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. In the management console, 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. In the management console, 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. In the management console, 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 home screen layout for supervised iOS devices

1. In the management console, 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 add (for example, **Built-in apps**).
5. Drag and drop the app icons from the list to the home screen, dock, or folder.
6. Click **Add**.

Manage app notifications on supervised 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.

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.

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. In the management console, 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.
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. In the **Show previews** drop-down list, select one of the following options:
    - **Always**: Notifications always include previews.
    - **When unlocked only**: Notifications include previews only when the device is unlocked.
    - **Never**: Notifications never include previews.
12. 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 Apple CarPlay. This setting applies only to iOS 12.0 and later devices.
13. Click **Save**.
14. Repeat steps 4 to 13 to add additional per-app notifications.
15. 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.

Customize 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.

When you change the icon, it is updated on all activated iOS devices.

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

1. In the management console, on the menu bar, click **Settings**.
2. In the left pane, expand **App management**.
3. Click **Work Apps app for iOS**.
4. Do one of the following:

Task	Steps
Customize the Work Apps icon.	**a.** In the **Name** field, type a name for the custom icon. The name appears on the device just under the icon. **b.** Click **Browse**. Locate and select an image for the Work Apps icon. The supported image formats are .png, .jpg, or .jpeg. Avoid using transparent elements. Transparent elements display as black on the device. **c.** To let users toggle the Work Apps icon from regular to full screen mode, select **Display the Work Apps app in full screen mode**. **d.** Click **Save**.
Remove the Work Apps icon.	You might remove the Work Apps icon if users use the BlackBerry Dynamics Launcher. **a.** Click **Disable Work Apps app**. **b.** Click **Disable**.

5. Click **Save**.

Managing Android devices with OEM app configurations

BlackBerry UEM supports Android OEMConfig apps, which allow you to use app configurations to manage device manufacturer APIs. Many Android devices, including devices from Samsung, have proprietary APIs on the device. UEM provides the ability to manage settings controlled by Knox Platform for Enterprise and BlackBerry APIs using profiles and IT policy rules. However, other Android device manufactures may also have device-specific APIs with settings that they want administrators to manage. To provide this functionality, the manufacturer can provide an OEMConfig app for devices that allows administrators to manage device features through app configuration settings.

Samsung provides the Knox Service Plugin app to allow configuration of Knox Platform for Enterprise devices. The Knox Service Plugin (KSP) is the Samsung OEMConfig-based solution that allows you to use Knox Platform for Enterprise management features on your EMM solution. For more information about setting up KSP in UEM, see Create a Knox Service Plugin profile.

Minimum device requirements for KSP: A version of Android and Knox that UEM supports.

For more information about KSP, see the information from Samsung.

To download the KSP app, visit Google Play.

If you choose to use the Knox Service Plugin, consider the following:

- Samsung devices don't give precedence to either the Knox Service Plugin or UEM IT policies and profiles. The device uses the most recent settings it receives.
- Samsung recommends using UEM to manage Samsung specific options where possible and using the Knox Service Plugin to manage only settings that can't be configured in UEM in another way (for example, recent updates to Samsung device capabilities that can't yet be managed by your version of UEM).
- If you use the Knox Service Plugin, ensure that the app configuration settings match the behavior configured in the IT policy and profiles also sent to the device to avoid inconsistent device behavior.

For more information about Android Enterprise OEMConfig, visit http://www.appconfig.org/android.html.

Create a Knox Service Plugin profile

You can enable the Knox Service Plugin, add the app, and manage the KSP profile settings.

1. In the management console, on the menu bar, click **Policies and profiles > Policy > Knox Service Plugin**.
2. In the **Enable Knox Service Plugin** dialog box, click **Enable**.

   The Knox Service Plugin app is added to the app list automatically.
3. On the **Knox Service Plugin profile** page, click +.
4. Specify a name for the profile.
5. Specify settings for the profile.
6. Click **Save**.

The policy that you created now appears in the App configuration table for the Knox Service Plugin app in the app list.

Get your organization’s enterprise ID for pre-release apps in Google Play

Google Play allows developers to create tracks for pre-release apps (for example, a beta track) and target those tracks to specific enterprises. If your organization uses pre-release apps, you will need to provide your organization's enterprise ID to the app developers to access them.

Before you begin: Configure Android Enterprise.

1. In the management console, on the menu bar, click **Settings > External Integration > Android & Chrome Management**. The enterprise ID is displayed under **Enterprise ID**.
2. Give the enterprise ID to your organization's app developer to add to the Google Play developer account. For more information, see Play Console Help: Set up an open, closed, or internal test.

Appendix: App behavior

The following sections describe the app behavior on devices based on activation types and app dispositions.

App behavior on iOS devices with MDM controls activations

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have assigned the "Feature - BlackBerryApp Store" entitlement to the user. For more information, see Add the work app catalog to the BlackBerry Dynamics Launcher.

For iOS and iPadOS devices activated with MDM controls, 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	On supervised devices, apps are installed automatically. If the app is already installed, the app becomes managed by UEM. On non-supervised devices, user is prompted to install apps. If apps are already installed, user is prompted to allow UEM to manage the apps. 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. You can use a compliance profile to define the actions that occur if required apps are not installed.	iTunes notifies users of available updates. Apps are removed from the "New/ Updated" list when the user updates the app. (can take up to one hour) For devices that don't have access to iTunes, users aren't notified but can download the update from the app catalog if the device is assigned an Apple VPP license.	Apps are automatically removed without notification. Apps no longer appear in the app catalog.	Apps are removed automatically.

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	If apps are already installed on supervised devices, the app becomes managed by UEM. On non-supervised devices, user is prompted to allow UEM to manage the apps. User is notified of a change to the app catalog. Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed). Users can choose whether to install the apps.	iTunes notifies users of available updates. Apps are removed from the "New/Updated" list when the user views the details (whether or not the app is updated).	Apps are automatically removed without notification. Apps no longer appear in the app catalog.	Apps are removed automatically.

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	On supervised devices, apps are installed automatically. If the app is already installed, the app becomes managed by UEM. On non-supervised devices, user is prompted to install apps. If apps are already installed, user is prompted to allow UEM to manage the apps. If the user cancels the installation, they can install apps from the app catalog. 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. You can use a compliance profile to define the actions that occur if required apps are not installed.	Apps are removed from the "New/ Updated" list when the user updates the app.	Apps are automatically removed without notification. Apps no longer appear in the app catalog.	Apps are removed automatically.

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	If apps are already installed on supervised devices, the app becomes managed by UEM. On non-supervised devices, user is prompted to allow UEM to manage the apps. 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.	Apps are removed from the "New/ Updated" list when the user updates the app.	Apps are automatically removed from devices activated with MDM controls without notification. Apps are not removed from devices activated with User privacy. Apps no longer appear in the app catalog.	Apps are removed automatically.

For information about prompt behavior of installing apps, see Add an iOS app to the app list.

App behavior on iOS devices with User privacy activations

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have if you have assigned the "Feature - BlackBerryApp Store" entitlement to the user. For more information, see Add the work app catalog to the BlackBerry Dynamics Launcher.

When you activate iOS and iPadOS devices with User privacy, you can choose whether to allow app management. If you allow app management, app behavior for User privacy activations is the same as for MDM controls activations. If you don't allow app management for devices activated with 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	The user isn't prompted to install apps. User must go to the app catalog to install the required apps. 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.	iTunes notifies users of available updates. Apps are removed from the "New/Updated" list when the user updates the app. (can take up to one hour) For devices that don't have access to iTunes, users aren't notified but can download the update from the app catalog.	Apps remain on the device. Apps no longer appear in the app catalog.	Apps remain on the device.
Public apps with an optional disposition	If app is already installed, nothing happens. User is notified of a change to the app catalog. Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed). Users can choose whether to install the apps.	iTunes notifies users of available updates. Apps are removed from the "New/Updated" list when the user views the details (whether or not the app is updated).	Apps remain on the device. Apps no longer appear in the app catalog.	Apps remain on the device.

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	If apps are already installed, user is prompted to allow UEM to manage the apps. 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.	Apps are removed from the "New/ Updated" list when the user updates the app.	Apps remain on the device. Apps no longer appear in the app catalog.	Apps remain on the device.
Internal apps with an optional disposition	If apps are already installed, nothing happens. 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.	Apps are removed from the "New/ Updated" list when the user updates the app.	Apps remain on the device. Apps no longer appear in the app catalog.	Apps remain on the device.

For information about prompt behavior of installing apps on a device, see Add an iOS app to the app list.

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 if you have assigned the "Feature - BlackBerry App Store" entitlement to the user. For more information, see Add the work app catalog to the BlackBerry Dynamics Launcher.

For Android Enterprise devices (including Samsung Knox devices activated with Android Enterprise), 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 uninstalled on the device.	The work profile and assigned work apps are 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
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 uninstalled on 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 uninstalled on the device.	Apps are automatically removed from the device.
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 uninstalled on 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 uninstalled on 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 uninstalled on the device.	The work profile and assigned work apps are removed from the device.

You can specify update behavior for apps running the the foreground in the device SR requirements profile.

App behavior on Android devices without a work profile

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have if you have assigned the "Feature - BlackBerry App Store" entitlement to the user. For more information, see Add the work app catalog 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	User is notified of a change to the app catalog. 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. You can use a compliance profile to define the actions that occur if required apps are not installed.	User is notified by Google Play.	The user is prompted to remove the apps. Apps no longer appear in the app catalog.	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.	The user is prompted to remove the apps. Apps no longer appear in the app catalog.	The user is prompted to remove the apps.
Internal apps with a required disposition	User is notified of a change to the app catalog. Apps are installed automatically. Apps are removed from the "New/ Updated" list when the user views the details or when the app is installed. You can use a compliance profile to define the actions that occur if required apps are not installed.	User is notified of a change to the app catalog. Updates are installed automatically. Apps are removed from the "New/ Updated" list when the user views the details or when the app is updated.	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 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 Windows 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	Users can choose whether to install the apps. For offline apps, users install the app from the BlackBerry UEM App Catalog. Not supported on Windows 10 Mobile devices.	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	Users can choose whether to install the apps. For online apps, users install the app from the Windows Store app on their devices. Not supported on Windows 10 Mobile devices.	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 Samsung Knox devices

For devices enabled for BlackBerry Dynamics, the work app catalog appears in the BlackBerry Dynamics Launcher if you have if you have assigned the "Feature - BlackBerryApp Store" entitlement to the user. For more information, see Add the work app catalog to the BlackBerry Dynamics Launcher.

Note: Samsung Knox activation types will be deprecated in a future release. Devices that support Knox Platform for Enterprise can be activated using the Android Enterprise activation types. For more information, see KB 54614.

For Samsung Knox devices activated with "MDM controls" (not Android Enterprise), 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	The user is prompted to install the apps. 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. You can use a compliance profile to define the actions that occur if required apps are not installed.	Google Play notifies users of updates. App appears in the "New/Updates" list.	The user is prompted to uninstall the apps.	The user is prompted to uninstall assigned work apps
Public apps with an optional disposition	The user can choose whether to install the apps. 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.	Google Play notifies users of updates. App appears in the "New/Updates" list.	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	User can choose whether to install the apps. User installs apps from the BlackBerry UEM Client.	User can choose whether to update the apps. User updates apps from the BlackBerry UEM Client.	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	All public apps are restricted by default in the work space. The user is prompted to install the apps. 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. You can use a compliance profile to define the actions that occur if required apps are not installed.	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	All apps are restricted by default in the work space. Assigned apps are shown in the BlackBerry UEM Client, but they must be installed from Google Play. Google Play must be enabled in the IT policy that is assigned to the user.	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	Users can choose whether to install the apps. Users install apps from the BlackBerry UEM Client and apps are installed in the work space.	Users can choose whether to update the apps. Users update app from the BlackBerry UEM Client.	Apps are automatically removed from the device.	The work space is removed and the apps remain in the personal space.

Legal notice

Patents, as applicable, identified at: www.blackberry.com/patents.

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
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada