# BlackBerry UEM

## Managing apps

Administration

12.14

# Contents

# Apps

You can create a library of apps that you can manage, deploy, and monitor on  devices. To manage and deploy apps, you add the apps to the app list in BlackBerry UEM and assign them to user accounts, user groups, or device groups.

When you manage apps, you perform the following actions:

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

You can also specify whether apps are required or optional and, depending on the device and activation type, restrict apps from being installed on devices.

# Adding apps to the app list

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

**Note:** If your organization uses Microsoft Intune for 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 online store, the Google Play store, the Windows Store, or the BlackBerry World storefront.

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, visit support.blackberry.com/community to read article 52777.

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

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

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

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

10. In the **Supported device form factor** drop-down list, select the form factors that the app can be installed on. For example, you can prevent the app from being available in the Work Apps app for iPad.
11. If you want the app to be deleted from the device when the device is removed from BlackBerry UEM, select **Remove the app from the device when the device is removed from BlackBerry UEM**. This option applies only to apps with a disposition marked as required and the default installation for required apps is set to prompt once.
12. If you want to prevent apps on iOS devices from being backed up to the iCloud online service, select **Disable iCloud backup for the app**. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.
13. In the **Default installation for required apps** drop-down list, perform one of the following actions:
    - If you want users to receive a prompt to install the app on their iOS devices, select **Prompt once**. If users dismiss the prompt, they can install the app later using the Work Apps screen in the BlackBerry UEM Client app or the Work Apps icon on the device.
    - If you don't want users to receive a prompt, select **No prompt**.

    If users dismiss the prompt or don't receive a prompt, they can install the app using the Work Apps screen in the BlackBerry UEM Client app or the Work Apps icon on the device. 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.
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**.<br>2. Click **Browse** and select the template that you want to add.<br>3. Click **Upload**.<br>4. For each setting, enter the value that you want to set.<br>For more information about app configuration .xml templates, visit http://www.appconfig.org/ios/. |
| Copy another app configuration | 1. Click + > **Copy from an app configuration**.<br>2. In the **Copy from** drop-down list, select the app configuration that you want to copy.<br>3. For each setting, edit the key name or value. |
| Create an app configuration manually | 1. Click + > **Configure manually**.<br>2. For each setting that you want to add, click + and select a value type for the setting.<br>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 BlackBerry UEM console. If your organization is using a proxy server, you must ensure that no SSL interception occurs. For more information on ports that must be open, visit support.blackberry.com/community to read article 52777. For more information about configuring BlackBerry UEM to support Android Enterprise devices, see the on-premises Configuration content or the Cloud Configuration content.

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

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

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

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. In the left navigation menu, click .
5. Search for the app that you want to add or pick an app on the store home page.
6. Select the app.
7. Click **Approve**.
8. To accept app permissions on behalf of users, click **Approve**. You must accept the app permissions to allow required apps to be automatically installed on Android Enterprise devices or in Knox Workspace. If you don't accept the app permissions on behalf of users, the app can't be managed in BlackBerry UEM.
9. On the **Approval Settings** tab, choose how you would like to handle new app permission requests when there is an updated app.
   - To automatically accept the new permissions added by the app vendor, select **Keep approved when app requests new permissions**.
   - To manually re-accept the new app permissions added by the app vendor before the app can be sent to new devices, select **Revoke app approval when this app requests new permissions**. For more information about updating app permissions, see Update app permissions for Android Enterprise apps.
10. If you selected the **Revoke app approval when this app requests new permissions** option on the Notifications tab, add a subscriber to be notified when the app permission changes. The administrator will have to re-approve the app before users can access it.
11. Click **Done**.
12. In the **App description** field, type a description for the app.
13. 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.
14. To control runtime app permissions, click **Set app permissions**. For each permission, choose one of the following:

- Grant
- Deny
- Use app permission policy

15. Click **Save**.
16. 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**.
17. If you want the app to update automatically on Android Enterprise devices, select **Automatically update app on Android Enterprise devices when update available**.
18. 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.
19. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

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

20. 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**.
21. Click **Add**.

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

If BlackBerry UEM is not configured to support Android Enterprise, use the following procedure.

If BlackBerry UEM is configured to support Android Enterprise devices, see Add an Android app to the app list.

1. 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 | **a.** In the drop-down list, select a category. |
| Create a category for the app | **a.** Type a name for the category. The new category will appear in the drop-down list with the "new category" label beside it<br>**b.** Press **Enter**.<br>**c.** Press **Enter**. |

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

## Add a Windows 10 app to the app list

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

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

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

**Before you begin:**

- If you have an on-premise environment, Specify the shared network location for storing internal apps to store offline apps.
- Configure BlackBerry UEM to synchronize with the Windows Store for Business

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

#### Configuring BlackBerry UEM to synchronize with the Windows Store for Business

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

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

When you configure BlackBerry UEM to synchronize with the Windows Store for Business, you perform the following actions:

| Step | Action |
|---|---|
| 1 | Create a Microsoft Azure account. For more information, see the on-premises Configuration content or the Cloud Configuration content. |
| 2 | Synchronize Microsoft Active Directory with Microsoft Azure. For more information, see the on-premises Configuration content or the Cloud Configuration content. |
| 3 | Create an enterprise endpoint in Azure. For more information, see the on-premises Configuration content or the Cloud Configuration content. |
| 4 | Configure BlackBerry UEM to synchronize with the Windows Store for Business. |
| 5 | Create an administrator for the Windows Store for Business. |
| 6 | Activate the app in the Windows Store for Business. |

#### Configure BlackBerry UEM to synchronize with the Windows Store for Business

**Before you begin:** Create an enterprise endpoint in Azure.

1. Log in to the BlackBerry UEM management console.
2. Go to **Settings > App management > Windows 10 apps**.
3. Enter the information you copied from the Azure portal when you created the enterprise application in Azure.

- **Client ID**: The Application ID generated by the Azure application registration
- **Client key**: The client secret generated by the Azure application registration
- **OAUTH 2.0 token endpoint**: The tenant specific OAuth endpoint URL for requesting authentication tokens
- **Username**: The administrator username for BlackBerry UEM to access Intune
- **Password**: The password for the username

4. Click **Next**.

**After you finish:** Create an administrator for the Windows Store for Business.

#### Create an administrator for the Windows Store for Business

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

**Before you begin:**

- Configure BlackBerry UEM to synchronize with the Windows Store for Business.

1. In the Microsoft Azure portal, go to **Microsoft Azure > Azure Active Directory > Users and groups > All users**.
2. Click **Add a user**.
3. On the screen, enter the required user information.
4. Click the arrow next to **Directory role** and select **Global administrator**, then click **OK**.
5. Create a password or select **Show Password** and copy the generated password.
6. Click **Create**.
7. Click **Azure Active Directory > Enterprise applications > All applications** and select the enterprise application you created.
8. Add the global administrator account you created as a user of the application.

**After you finish:** Activate the app in the Windows Store for Business.

#### Activate the app in the Windows Store for Business

**Before you begin:**

- Configure BlackBerry UEM to synchronize with the Windows Store for Business.
- Create an administrator for the Windows Store for Business

1. Log in to the Windows Store for Business using the Global Admin account you created.
2. Click **Manage > Settings > Distribute**.
3. Click **Add Management tool**.
4. Choose the app that you created to be the MDM tool you want to synchronize with the Windows Store for Business.
5. Click **Activate.**

#### Allowing users to install online Windows 10 apps

To allow users to install online Windows 10 apps, the user must exist in your Microsoft Azure directory, and the user's email address in BlackBerry UEM must match the user's email address in Microsoft Azure AD. You can synchronize your directory to Microsoft Azure using Microsoft Azure AD Connect. For instructions, see the on-premises Configuration content or the Cloud Configuration content.

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

#### Add an app category for a Windows 10 app

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

**Before you begin:** Add a Windows 10 app to the app list.

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

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

4. Click **Save**.

### Add a BlackBerry 10 app to the app list

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

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

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

# Adding internal apps to the app list

Internal apps include proprietary apps developed by your organization and apps made available for your organization's exclusive use. Internal apps are not added to BlackBerry UEM from public app storefronts.

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

If you are adding intermal apps in an on-premises environment, you must first Specify the shared network location for storing internal apps.

Users can find internal apps on their devices as follows:

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

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. 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

Follow this procedure to add internal apps for all devices. For Android Enterprise devices you can instead host new apps in Google Play. For more information, see Adding internal apps for Android Enterprise devices.

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

1. On the menu bar, click **Apps**.
2. Click  .
3. Click **Internal apps**.
4. Click **Browse**. Navigate to the app that you want to add or update.

5. Click **Open**.
6. Click **Add**.
7. Optionally, add a vendor name and an app description.
8. To add screen shots of the app, click **Add**. Browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
9. If you are adding an iOS app, perform the following actions:
   a) In the **Supported device form factor** drop-down list, select the form factors that the app can be installed on. For example, you can prevent the app from being available in the Work Apps app for iPad.
   b) If you want the app to be deleted from the device when the device is removed from BlackBerry UEM, select **Remove the app from the device when the device is removed from BlackBerry UEM**. This option applies only to apps with a disposition marked as required and the default installation for required apps is set to prompt once.
   c) If you want to prevent apps on iOS devices from being backed up to the iCloud online service, select **Disable iCloud backup for the app**. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.
   d) In the **Default installation method for required apps** drop-down list, if you want users to receive one prompt to install the app on their iOS devices, select **Prompt once**. If users dismiss the prompt, they can install the app later from the Work Apps list in the BlackBerry UEM Client app or the Work Apps icon on the device.
10. If you are adding an Android app, you can set runtime app permissions for the app. Click **Set app permissions**and for each permission that the app requests, specify whether to grant or deny permission or use the app permission policy, then click **Save**.
11. 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.
12. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

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

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

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

**After you finish:** If you are adding an app for Android Enterprise devices, complete one of the following tasks:

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

#### Update an internal app

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

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

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

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

### Adding an internal app for Android Enterprise devices

For Android Enterprise devices you can host new apps in Google Play.

You can add internal apps to Android Enterprise devices in three ways. The method you chose depends on your organization's needs.

| Option | Description |
|---|---|
| Add a private app to the app list for Android Enterprise devices | Use this option to quickly host a new internal app in Google Play. This is the recommended method for adding internal apps. This option supports only Android Enterprise devices. If you want to make the app available to other Android devices, you must use one of the other options in addition to or instead of this option. This option doesn't require you to purchase a developer account from Google. |
| Host an internal app for Android Enterprise devices in Google Play using the .apk file | This method involves using the Google Play App Developer portal, and requires the purchase of a developer account from Google. |
| Host an internal app for Android Enterprise devices in BlackBerry UEM using a .json file | Use this method to add internal apps if you don't want to upload apk. files to Google Play. When you use this method, the file is stored by BlackBerry UEM. Note that this method is available only when the 'Add Google Play account to work space' option is not selected in the activation profile that is assigned to the user. |

#### Add a private app to the app list for Android Enterprise devices

Use these instructions to add internal apps to Google Play to deploy to Android Enterprise devices.

Private apps display the symbol and your Android Enterprise Organization Name in the Vendor field in the app list.

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

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. In the left navigation menu, click .
5. Click .
6. In the **Title** field, type the text that will display on the device.
7. 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 BlackBerry UEM that the app is ready. When UEM receives the apk file, it adds the app to the app list automatically.
9. To add a description or icon for the the app or specify app details in Google Play, click **Make advanced edits**, login to Google Play, and make the required changes.
10. In the **Private apps** tab, click the app you added, then click **Select**.
11. In the **App description** field, type a description for the app.
12. To add screen shots of the app, click **Add** and browse to the screen shots. The supported image types are .jpg, .jpeg, .png, or .gif.
13. If you want the app to update automatically on Android Enterprise devices, select **Automatically update app on Android Enterprise devices when update available**.
14. For apps that support configuration settings, an **App configuration** table is displayed. If you want to create an app configuration, complete the following steps:
    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.
15. To filter apps in the app list by category and to organize the apps into categories in the work apps list on users' devices, you can select a category for the app. In the **Category** drop-down list, do one of the following:

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

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

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

**17.** Click **Add**.

**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.

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

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

**Before you begin:**

- You need an account to log in to the Google Developers Console. If Android Enterprise is configured, use the same email address for the developer account that you used to set up the work profile. For each BlackBerry UEM domain you need a different developer account.

For instructions on uploading an .apk file for Android Enterprise devices in the Google Developers Console, see the information from Google.

For more information, see Add an Android app to the app list.

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

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

**Before you begin:**

- Verify that you have OpenSSL, JDK, Python 2.x, and Android Asset Packaging Tool (aapt) installed in a Path location on the computer.
- You need an account to log in to the Google Developers Console. If you configured support for Android Enterprise, use the same email address for the developer account that you used to set up Android Enterprise. For each BlackBerry UEM domain you need a different developer account.
- In BlackBerry UEM, Add an internal app to the app list. Select the **Enable the app for Android Enterprise** option, and in the **App will be hosted by** drop-down list, click **BlackBerry UEM**. Copy and save the URL that is displayed in BlackBerry UEM.
  **Note:** You need to select **Enable the app for Android Enterprise** even if you are hosting the app for all Android devices.

For more information, see the information from Google.

#### 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.

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

2. Click .
3. Click **Google Play**.
4. In the left navigation menu, click .
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**.

# Adding web shortcuts to devices

You can shortcuts to web pages to iOS, macOS, and Android devices in a similar way to adding apps. For example, you can add a shortcut to your organization's internal website. How you add the shortcut depends on the device type.

For iOS and macOS devices, and for Android devices that aren't activated to use Android Enterprise, you add an app shortcut. The shortcut information and icon file are added to UEM.

For Android Enterprise devices, you add a Web app to Google Play. 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". Google web apps display the  symbol and your Android Enterprise Organization Name in the Vendor field in the app list.

## Create an app shortcut for iOS, macOS, and Android devices

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

**Before you begin:**

- Verify that users are assigned an app entitlement for "Feature – BlackBerry App Store" (com.blackberry.feature.appstore).
- Verify that the image that you plan to use as the icon for the shortcut meets the following requirements:
  - The image format is .png, .jpg, or .jpeg.
  - The image does not have transparent elements. Any transparent elements will display as black on the device.
  - The maximum image size is 120x120.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **App shortcut**.
4. Type a name and description for the app shortcut. The name is used as the label for the app shortcut.
5. Beside the **Shortcut icon** field, click **Browse**. Locate and select an image for the app shortcut icon. The supported image formats are .png, .jpg, or .jpeg.
6. Select the device types that you want to configure this app shortcut for.
7. In each of the device type tabs that you selected, in the URL field, type the web address of the shortcut. The web address must begin with http:// or https://.:

8. Select the location where you want the shortcut to be added. If you add the shortcut to the BlackBerry Dynamics Launcher, specify whether you want the web site to open in the BlackBerry Access browser.
9. Click **Add**.

## Create a web app for Android Enterprise devices

You create a web app for each shortcut that you want to display on users' Android Enterprise devices.

**Before you begin:**

Verify that the image that you plan to use as the icon for the shortcut is 512px x 512px and in .png, .jpg, or .jpeg format.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. In the left navigation menu, click .
5. Click .
6. In the **Title** field, type the text that will display on the device.
7. In the **URL** field, type the web address of the shortcut. The web address begins with https://.:
8. Select whether you want the web app to display full screen, standalone, or with minimal UI.
9. Click **Upload icon** and browse for the icon that you want to use for the web app.
10. Click **Create**.

    The web app is created in Google Play. Google Play takes several minutes to create the .apk file and send it to BlackBerry UEM. When UEM receives the apk file, it adds the web app to the app list automatically.

**After you finish:** After the web app appears in the app list, you can update the BlackBerry UEM app settings as you would for any other internal app for Android Enterprise devices.

## Update a web app for Android Enterprise devices

You can update web apps that you have added to Google Play. When you update the Web app, Google Play creates an updated version of the .apk file and sends it to BlackBerry UEM. BlackBerry UEM treats the updated .apk file in the same manner as new versions of other apps for Android Enterprise devices.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Google Play**.
4. In the left navigation menu, click .
5. Click the web app that you want to update.
6. Click **Edit**.
7. Update the settings as needed.
8. Click **Save**.

    The web app is updated in Google Play. Google Play takes several minutes to create the new .apk file and send it to BlackBerry UEM. When UEM receives the apk file, it updates the app list automatically. If the app is not added to the app list as expected, click **Select** to manually add the app to the app list.

**After you finish:** After the updated web app appears in the app list, you can update the BlackBerry UEM app settings as you would for any other internal app for Android Enterprise devices.

# Adding or changing an app configuration

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

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

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

BlackBerry UEM also supports Android OEMConfig apps, which allow you to use app configurations to manage device manufacturer APIs.

For information about app settings, contact the app vendor.

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

## Managing Android devices with 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 and BlackBerry have proprietary APIs on the device. BlackBerry 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 Samsung's OEMConfig based solution that enables IT administrators to use Knox Platform for Enterprise management features on their EMM solution. For more information about setting up KSP in BlackBerry UEM, refer to the information from Samsung:

- Add KSP to BlackBerry UEM
- Configure policies for KSP
- Assign the KSP app

Minimum device requirements for KSP: Android 9 or later (Knox 3.2.1 or later).

For more information about KSP, refer to the information from Samsung.

To download the KSP app, visit Google Play.

If you choose to use Knox Service Plugin, be aware of the following considerations:

- Samsung devices don't give precedence to either Knox Service Plugin or BlackBerry 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 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 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 OEM Config, visit http://www.appconfig.org/android-oemconfig/.

# Obtain your organization's enterprise ID for Google Play app tracking

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 is using this feature, you will need to provide your organization's enterprise ID to the app developer.

UEM management console, navigate to **Settings > External Integration > Android Enterprise**. The enterprise ID is displayed under **Enterprise ID**.
The app developer will use the enterprise ID in the Google Play developer account under App > Testing > Manage track > Testers tab > Manage organizations.

# Preventing users from installing specific apps

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

#### Restrict specific apps

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

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

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

#### Allow specific apps

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

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

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

For more information about creating compliance profiles, see Create a compliance profile.

# Steps to prevent users from installing specific apps

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

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

# Add an app to the restricted app list

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

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

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

| Task | Steps |
| --- | --- |
| Add an iOS app to the restricted list | a. Click **App Store**.<br>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.<br>c. Click **Search**.<br>d. In the search results, click **Add** to add an app. |
| Add an Android app to the restricted list | a. Click **Google Play**.<br>b. In the **App name** field, type the app name.<br>c. In the **App web address from Google Play** field, type the web address of the app in Google Play.<br>d. Click **Add** to add the app or click **Add and new** to add another app after you add the current one. |

# Managing apps on the app list

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

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

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

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

Apps listed with a lock icon are BlackBerry Dynamics apps. For more information, see Managing BlackBerry Dynamics apps.

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

## Delete an app from the app list

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

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

## Change whether an app is required or optional

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

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

# Device notifications for new and updated apps

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

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

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

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

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

For more information about app notifications, see:

- App behavior on iOS devices with MDM controls activations
- App behavior on iOS devices with User privacy activations
- App behavior on Android Enterprise devices
- App behavior on Android devices without a work profile
- App behavior on Samsung Knox devices

# 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 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 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.<br><br>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.<br><br>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.<br><br>You can use a compliance profile to define the actions that occur if required apps are not installed. | iTunes notifies users of available updates.<br><br>Apps are removed from the "New/Updated" list when the user updates the app. (can take up to one hour)<br><br>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.<br><br>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.<br>User is notified of a change to the app catalog.<br>Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed).<br>Users can choose whether to install the apps. | iTunes notifies users of available updates.<br>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.<br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Apps are not removed from devices activated with User privacy.<br><br>Apps no longer appear in the app catalog. | Apps are removed automatically. |

# 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 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 iOS 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.<br>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.<br>Apps are removed from the "New/Updated" list when the user updates the app. (can take up to one hour)<br>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.<br>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.<br>User is notified of a change to the app catalog.<br>Apps are removed from the "New/Updated" list only when the user views the details (whether or not the app is installed).<br>Users can choose whether to install the apps. | iTunes notifies users of available updates.<br>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.<br>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.<br>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.<br>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.<br>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.<br>Apps no longer appear in the app catalog. | Apps remain on the device. |

# 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, the following behavior occurs:

| App type | When the app is assigned to a user | When apps are updated | When the app is unassigned from a user | When the device is removed from BlackBerry UEM |
|---|---|---|---|---|
| Public apps with a required disposition | Apps are automatically installed. | Apps are automatically updated. | Apps are automatically removed from the device. | The work profile and assigned work apps are removed from the device. |

| 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.<br>Apps appear in Google Play for Work. | Google Play for Work notifies users about updates. | Apps are automatically removed from the device. | The work profile and assigned work apps are removed from the device. |
| Internal apps with a required disposition hosted in BlackBerry UEM | Supported only for Work space only devices.<br>Apps are automatically installed. | Supported only for Work space only devices.<br>Apps are automatically installed. | Apps are automatically removed from 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.<br>Apps appear in Google Play for Work. | Google Play for Work notifies users about updates. | Apps are automatically removed from the device. | The work profile and assigned work apps are removed from the device. |
| Internal apps with a required disposition hosted in Google Play | Apps are automatically installed on the device. | Google Play for Work notifies users about updates. | Apps are automatically removed from the device. | The work profile and assigned work apps are removed from the device. |
| Internal apps with an optional disposition hosted in Google Play | The user can choose whether to install the apps.<br>Apps appear in Google Play for Work. | Google Play for Work notifies users about updates. | Apps are automatically removed from the device. | The work profile and assigned work apps are removed from the device. |

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 - BlackBerryApp Store" entitlement to the user. For more information, see Add the work app catalog to the BlackBerry Dynamics Launcher.

**Note:** The MDM controls activation type is deprecated for devices with Android 10. For more information, visit https://support.blackberry.com/community to read article 48386.

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.<br>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.<br>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.<br>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.<br>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.<br>Apps are installed automatically.<br>Apps are removed from the "New/ Updated" list when the user views the details or when the app is installed.<br>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.<br>Updates are installed automatically.<br>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.<br>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.<br>Apps appear in the "New/Updated" list. | Apps appear in the "New/Updated" list. | The user is prompted to remove the apps.<br>Apps no longer appear in the app catalog. | The user is prompted to remove the apps. |

# 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, visit https://support.blackberry.com/community to read article 54614.

For app behavior on Samsung Knox devices activated with Android Enterprise activation types, see App behavior on Android Enterprise devices.

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

| App type | When the app is assigned to a user | When apps are updated | When the app is unassigned from a user | When the device is removed from BlackBerry UEM |
|---|---|---|---|---|
| Public apps with a required disposition | The user is prompted to install the apps.<br>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.<br>You can use a compliance profile to define the actions that occur if required apps are not installed. | Google Play notifies users of updates.<br>App appears in the "New/Updates" list. | The user is prompted to uninstall the apps. | The user is prompted to uninstall assigned work apps |

| 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.<br>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.<br>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.<br>User installs apps from the BlackBerry UEM Client. | User can choose whether to update the apps.<br>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 space only (Samsung Knox), the following behavior occurs:

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

| 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 a required disposition | Apps are automatically installed on devices. The user cannot uninstall the apps. | Apps are automatically updated on the device. | Apps are automatically removed from the device. | Apps are automatically removed from the device. |
| Internal apps with an optional disposition | Users can choose whether to install the apps.<br>Users install the apps from the BlackBerry UEM Client. | Users can choose whether to install the apps.<br>Users install the 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.<br>The user is prompted to install the apps.<br>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.<br>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. |

| 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 | All apps are restricted by default in the work space.<br>Assigned apps are shown in the BlackBerry UEM Client, but they must be installed from Google Play.<br>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. |
| Internal apps with an optional disposition | Users can choose whether to install the apps.<br>Users install apps from the BlackBerry UEM Client and apps are installed in the work space. | Users can choose whether to update the apps.<br>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. |

# App behavior on Windows 10 devices

| App type | Behavior when apps are assigned to a user | Behavior when apps are unassigned from a user | Behavior when devices are removed from BlackBerry UEM |
|---|---|---|---|
| Offline Windows Store apps with a required disposition | The apps are automatically installed on devices. Users cannot uninstall the apps. | The apps are automatically removed from devices. | The apps are automatically removed from devices. |

| 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 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.<br>For offline apps, users install the app from the BlackBerry UEM App Catalog.<br>Not supported on Windows 10 Mobile devices. | Users are not prompted to uninstall the apps. | Users are not prompted to uninstall assigned apps. |
| Online Windows Store apps with an optional disposition | Users can choose whether to install the apps.<br>For online apps, users install the app from the Windows Store app on their devices.<br>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 BlackBerry devices

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

| App type | Behavior when apps are assigned to a user | Behavior when apps are unassigned from a user | Behavior when the device is removed from BlackBerry UEM |
|---|---|---|---|
| Public apps with a required disposition | Not supported. | Not supported. | Not supported. |

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

# Viewing app feedback

BlackBerry UEM can receive and display error and information feedback from Android apps. Only apps that display app configuration settings in UEM and that have been designed to provide feedback to administrators can send feedback to UEM. The feedback provided depends on the app.

You can see whether an app on a user's device has sent feedback to UEM in the list of apps assigned to a specific device or in the list of users that an app is assigned to. The Feedback column in the list displays the date and time of the last feedback and displays ⚠ if the feedback is the result of an app error.

## View feedback for all apps on a device

You can see which apps on a device have sent feedback to BlackBerry UEM and review the feedback for each app.

1. 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 the device tab.
5. Expand the **Apps** list.

   The **Feedback** column in the list displays the date and time of the last feedback for all apps that have sent feedback to UEM
6. Click the entry in the **Feedback** column to display all of the feedback that the app has sent to UEM from the device.

### View feedback from all installations of an app

You can see which device instances of an app have sent feedback to BlackBerry UEM and review the app feedback from each device.

1. On the menu bar, click **Apps**.
2. Click the app that you want to view feedback for.
3. Click the **Assigned to users** tab.

   The tab displays the list of users and devices that have the app assigned. The **Feedback** column in the list displays the date and time of the last feedback for all instances of the apps that have sent feedback to UEM.
4. Click an entry in the **Feedback** column to display all of the feedback that the app has sent to UEM from that 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 to increase efficiency and consistency when managing apps. For example, you can use app groups to group the same app for multiple device types, or to group apps for users with the same role in your organization.

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

### Create an app group

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

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

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

| Task | Steps |
| --- | --- |
| If you have added at least one VPP account | **a.** Click **Add**.<br>**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.<br>**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.<br>**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.<br>**e.** Click **Add**, then click **Add** again.<br>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.<br>**Note:** If you grant access to more licenses than you have available, the first users who access the available licenses can install the app. |

7. For iOS and Android apps, if there is an available app configuration, select the **App configuration** to assign to the app.
8. 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.
9. Click **Add**, then click **Add** again.

### Edit an app group

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

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

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

# View which apps are assigned to user groups

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

# Viewing and customizing the apps list

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

## Select the information to display in the apps list

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

## Filter the app list

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

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

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

# Update the app list

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

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

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

If you have not configured support for Android Enterprise, information about Google Play apps must be updated manually. Updating the app information does not mean that the app is updated on a user's device. Users receive update notifications for their work apps in the same way that they receive update notifications for their personal apps.

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

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

# Update app permissions for Android Enterprise apps

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

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

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

| Status | Steps |
|---|---|
| Reaccept app permissions | The app permissions have changed in the Google Play console. To be able to manage the app, you must reaccept the app permissions. To reaccept the permissions, complete the following steps:<br>**a.** Click **Reaccept app permissions**.<br>**b.** Click **Accept**. |
| Delete app from BlackBerry UEM | The app was unapproved from the Google Play console but was not removed from BlackBerry UEM. If you want to continue to manage this app on devices, you must approve the app in the Google Play console. If you no longer want to manage the app, complete the following steps:<br>**a.** Click **Delete app from BlackBerry UEM**.<br>**b.** Click **Delete**. |

| Status | Steps |
| --- | --- |
| Approve app in Google Play | The app was unapproved in the Google Play console. To be able to manage the app, you must approve the app in the Google Play console. To approve the app, complete the following steps:<br>**a.** Click **Approve app in Google Play**.<br>**b.** Accept the app permissions.<br>**c.** Click **Accept**. |
| App was added in Google Play and is being added to BlackBerry UEM | Apps that have been added to the Google Play for Work console, but not to BlackBerry UEM, are automatically synchronized to BlackBerry UEM when you update the app list. You do not have to perform any actions. |

4. Click **Close**.

# Accept app permissions for Android Enterprise apps

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

**Before you begin:**

- Update the app list.

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

# Managing apps protected by Microsoft Intune

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

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

To deploy apps protected by Intune, you must first configure the connection between UEM and Intune. For more information, see "Connecting BlackBerry UEM to Microsoft Azure" in the on-premises Configuration content or the UEM Cloud Configuration content.

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

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

## Configure BlackBerry UEM to synchronize with Microsoft Intune

**Before you begin:** Connect BlackBerry UEM to Microsoft Azure and create an enterprise endpoint in Azure. For more information see the, on-premises Configuration content or the UEM Cloud Configuration content.

**Note**: The Client Credentials authentication method has been removed in BlackBerry UEM 12.14 and later. For existing servers that have been upgraded to UEM 12.14, the administrator must take action to migrate the configuration to Modern Authentication.

1. Click **Settings > External Integration > Microsoft Intune**.
2. Enter the information you copied from the Azure portal when you created the enterprise application in Azure.
   - **Azure Tenant ID**: The ID of the Azure Active Directory where you registered the application
   - **Client ID**: The application ID generated by the Azure application registration
   - **Client key**: The client secret generated by the Azure application registration

   For more information see the, on-premises Configuration content or the UEM Cloud Configuration content.
3. Confirm the **Reply URL**. The **Reply URL** field is automatically populated with the web address of the BlackBerry UEM management console. This URL is required when you create the enterprise endpoint in Microsoft Azure . For more information see the on-premises Configuration content or the UEM Cloud Configuration content.

   **Note**: The Reply URL is automatically derived from the %AdminPortalURL%default variable. By default, this variable will be set to the first UEM Core server installed in the environment. This variable can be modified by going to Settings > General Settings > Default Variables. For more information, see the Administration content.
4. Click **Next**.

**After you finish:** Create a Microsoft Intune app protection profile

# Create a Microsoft Intune app protection profile

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

**Before you begin:**

- Configure the connection between BlackBerry UEM and Microsoft Intune according to the instructions in the on premises Configuration content or the UEM Cloud Configuration content. The Microsoft Intune app protection profile does not appear on the Policies and Profiles page if the connection isn't configured.
- For Android devices, ensure the Microsoft Company Portal app is installed on devices. For more information, see the Microsoft Intune documentation.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Microsoft Intune app protection profile**.
3. Click +.
4. Type a name and description for the profile.
5. Configure the appropriate values for each device type.
6. Click **Add**.

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

## Microsoft Intune app protection profile settings

Microsoft Intune app protection profiles are supported on the following device types:

- iOS
- Android

## Common: Microsoft Intune app protection profile settings

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 Office 365 apps, on the device.<br>To allow interoperability between BlackBerry Dynamics apps and Intune-managed apps, BlackBerry Enterprise BRIDGE must be installed on users' devices.<br>For more information, see the BlackBerry Enterprise BRIDGE Administration Guide |
| Custom JSON | Edit the JSON values to customize messages and warnings seen by your users in the BlackBerry Enterprise BRIDGE app. |
| **Data relocation** | |

| Intune app protection profile setting | Description |
|---|---|
| **Interoperability** | |
| Allow app to transfer data to other apps | This setting specifies the apps Intune-managed apps can send data to.<br>Possible values:<br>• Policy managed apps: This option allows data to be transferred only to other apps that are managed by Intune. This option is the default.<br>• All apps<br>• None<br>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.<br>Possible values:<br>• Policy managed apps: This option allows data to be transferred only from other apps that are managed by Intune. This option is the default.<br>• All apps<br>• None<br>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.<br>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:<br>• Local storage<br>• OneDrive for Business<br>• SharePoint |
| Restrict cut, copy, and paste with other apps | This setting specifies how cut, copy, and paste operations can be used with the app.<br>Possible values:<br>• Blocked: This option prevents cut, copy, and paste operations between this app and other apps.<br>• Policy managed apps: This option allows cut, copy, and paste operations between the app and other apps that are managed by Intune.<br>• 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.<br>• Any app: This option allows cut, copy, and paste operations between all apps on the device. |
| Disable contact sync | This setting specifies whether the app can save contacts to the native Contacts app on the device. |

| Intune app protection profile setting | Description |
|---|---|
| **Interoperability** | |
| Disable printing | This setting specifies whether the app can print data. |
| **Access** | |
| Require corporate credentials for access | This setting specifies whether users must use their organization credentials to access the app.<br>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.<br>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. |
| 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.<br>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. |

### 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.<br>Possible values:<br>• When device is locked: This option encrypts all app data when the device is locked.<br>• 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<br>• After device restart: This option encrypts app data when the device is restarted until the device is unlocked for the first time.<br>• Use device settings: This option encrypts app data according to the default settings on the device. This option requires users to set a password on the device. |
| Prevent iTunes and iCloud | This setting specifies whether app data can be backed up to iTunes or iCloud. |
| App package IDs | This setting specifies the package IDs of the apps that this profile applies to. You can enter the package ID or select from the list of available Intune-managed apps. |
| Restrict web content transfer with other apps | This setting specifies which browser opens web links in apps.<br>Possible values:<br>• Any app: The user can choose which app opens the web link.<br>• Intune Managed Browser: Web links can open in any browser managed by Intune.<br>• Microsoft Edge: Web links open in Microsoft Edge.<br>• BlackBerry Access: Web links open in BlackBerry Access.<br>• 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 operating system | Select this setting to specify a minimum iOS version to use this app. If the iOS version on the device does not meet the requirement, the user can't use the app. You can specify a single decimal point (for example, 12.0). |
| Require minimum iOS operating system (Warning only) | Select this setting to specify a minimum recommended iOS version to use this app. If the iOS version on the device does not meet the requirement, the user receives a notification that can be dismissed. You can specify a single decimal point (for example, 12.0). |

| Intune app protection profile setting | Description |
|---|---|
| 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).<br>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).<br>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. |

### 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. This setting is supported by Android 6.0 and later. |
| App package IDs | This setting specifies the package IDs of the apps that this profile applies to. You can enter the package ID or select from the list of available Intune-managed apps. |
| Restrict web content transfer with other apps | This setting specifies which browser opens web links in apps.<br>Possible values:<br>• Any app: The user can choose which app opens the web link.<br>• Intune Managed Browser: Web links can open in any browser managed by Intune.<br>• Microsoft Edge: Web links open in Microsoft Edge.<br>• BlackBerry Access: Web links open in BlackBerry Access.<br>• 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. |

| Intune app protection profile setting | Description |
|---|---|
| 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.<br>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.<br>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.<br>Specify the version using the date format YYYY-MM-DD. |
| 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.<br>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.<br>You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).<br>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.<br>You can specify up to four release identifiers. Separate release identifiers with periods (for example, 10.3 or 10.3.14.2).<br>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. |

# Wipe apps managed by Microsoft Intune

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

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

# Managing Apple VPP accounts

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

## Add an Apple VPP account

To see how to add an Apple VPP account, visit our YouTube channel.

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

## Edit an Apple VPP account

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

# Update Apple VPP account information

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

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

# Delete an Apple VPP account

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

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

# Assigning Apple VPP licenses to devices

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

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

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

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

## View Apple VPP license assignment

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

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

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

   - The number of available VPP licenses
   - The number of used VPP licenses
3. In the **Used licenses** column for the app, click the used licenses link.

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

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

4. Click **Close**.

# Limiting devices to a single app or apps that you specify

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

## Create an app lock mode profile

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

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

**Before you begin:** If you plan to use the app list to select an app, make sure that the app is available in the app list.

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

| Task | Steps |
|---|---|
| Specify the app to run on iOS devices | In the **Specify the app to run on the device** section, perform one of the following actions:<br>• Click **Select an app from the app list**, click **Add an app**, and click an app in the list.<br>• 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 (.).<br>• Click **Select a built-in iOS app** and select an app from the drop-down list. |

| Task | Steps |
| --- | --- |
| Specify the apps to run on Android devices | In the **Specify the apps to run on the device** section, beside the app table, click + and do the following to specify the apps that you want to limit the device to:<br>• 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**.<br>• Click **Select an app from the app list**, and click an app in the list. Click **Add**.<br>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. |
| Specify the app to run on Windows 10 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.<br>• 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`. |

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

**After you finish:** If necessary, rank profiles.

# Viewing personal app lists

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

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

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

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

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

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

## View the personal apps list in the management console

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

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

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

1. On the menu bar, click **Apps > Personal apps**.
2. In the **App name** column for the app, click the app name.

   For the specified app, you can view the corresponding app details on the public app storefront, when applicable.
3. In the **Installed #** column for the app, click the installed number.

   For the specified app, you can view the user account and the device that the app is installed on.

## Turn off personal apps collection

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

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

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

# Rating and reviewing apps

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

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

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

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

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

- BlackBerry 10 devices
- Android Enterprise devices

## Enable or disable app ratings and reviews for all apps

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

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

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

## Enable app ratings and reviews for existing apps

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

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

# View app reviews in the management console

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

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

# Specify app rating and review settings for multiple apps

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

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

# Delete app ratings and reviews

You can delete app ratings and reviews as required.

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

# Configure the layout of apps on iOS devices

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

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

# Managing notifications for apps on iOS devices

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

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

## Create a per-app notification profile

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

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

    This setting applies only to iOS 14.0 and later devices.
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.

# Managing the Work Apps icon for iOS devices

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

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

## Customize the Work Apps icon

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

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

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

- Image format must be .png, .jpg, or .jpeg.
- Avoid using .png images that have transparent elements. The transparent elements display as black on the device.
- For suggested image sizes, visit developer.apple.com to see Icon and Image Sizes.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **App management**.
3. Click **Work Apps app for iOS**.
4. In the **Name** field, type a name for the custom icon. The name appears on the device just under the icon.
5. Click **Browse**. Locate and select an image for the Work Apps icon. The supported image formats are .png, .jpg, or .jpeg.
6. Select **Display the Work Apps app in full screen mode** to let users toggle the Work Apps icon from regular to full screen mode.
7. Click **Save**.

## Disable the Work Apps app for iOS

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

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

# Set the organization name for BlackBerry World

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

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

# Legal notice

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