BlackBerry UEM

Activating devices

Administration

12.18

Contents

Device activation

When you or a user activates a device, the device is associated with BlackBerry UEM so that you can manage devices and users can access work data on their devices.

When a device is activated, you can send IT policies and profiles to control the available features and manage the security of work data. You can also assign apps for the user to install. Depending on how much control the selected activation type allows, you may also be able to protect the device by restricting access to certain data, remotely setting passwords, locking the device, or deleting data.

You can assign activation types to accommodate the requirements of devices owned by your organization and devices owned by users. Different activation types give you different degrees of control over the work and personal data on devices, ranging from full control over all data to specific control over work data only.

Activation types: iOS devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by iOS and iPadOS. A separate work space is not installed on the device and there is no added security for work data. You can control the device using commands and IT policies. During activation, users must install a mobile device management profile on the device. To specify whether BlackBerry UEM can limit activation by device ID, select **Allow only approved device IDs**.

Activation type	Description
User privacy	You can use the User privacy activation type to provide basic control of devices while making sure that users' personal data remains private. With this activation type, no separate container is installed on the device, and no added security for work data is provided. Devices activated with User privacy are activated on BlackBerry UEM and can use services such as Find my Phone and Root Detection, but administrators cannot control device policies. **Note:** For SIM-based licensing, you must select "Allow access to SIM card and device hardware information to enable SIM-based licensing" in the activation profile. Users must install an MDM profile that can access only the SIM card and device hardware information that is required to check if an appropriate SIM license is available (for example, ICCID and IMEI). This activation type is not supported for Apple TV devices. When you allow User privacy activations, you select the profiles that you want manage on the device based on the needs of your organization. You can choose any of the following: • **Allow access to SIM card and device hardware information to enable SIM-based licensing**: This option specifies whether BlackBerry UEM can access SIM card and device hardware information, such as iCCID and IMEI, to check if an appropriate SIM license is available. • **Allow App management**: This option specifies whether you want to install or remove work apps on the device, and display a list of installed work apps in the user details screen.You can also specify whether to allow app shortcuts. • **Allow IT Policy management**: This option specifies whether you want to apply a limited set of IT policy rules to the device (password policies, allow screenshots, allow documents from managed sources in unmanaged destinations, and allow documents from unmanaged sources in managed destinations). • **Allow Email profile management**: This option specifies whether to apply the Email profile settings that are assigned to the user to the device. • **Allow Wi-Fi profile management**: This option specifies whether to apply the Wi-Fi profile settings that are assigned to the user to the device. • **Allow VPN profile management**: This option specifies whether to apply the VPN profile settings that are assigned to the user to the device.
User privacy - User enrollment	You can use the User privacy - User enrollment activation type for iOS and iPadOS devices to make sure that user data is kept private and separated from work data. With this activation type, a separate work space is installed on the device for work apps and the native Notes, iCloud Drive, Mail (attachments and full email bodies), Calendar (attachments), and iCloud Keychain apps. This activation type enables app management, IT policy management, email profiles, Wi-Fi profiles, and per-app VPN. Administrators can manage work data (for example, wipe work data) without affecting personal data. This activation type is supported on unsupervised iPhone and iPad devices that run iOS and iPadOS 13.1 and later.

Activation type	Description
Device registration for BlackBerry 2FA only	This activation type supports the BlackBerry 2FA solution for devices that BlackBerry UEM does not manage. This activation type does not provide any device management or controls, but allows devices to use the BlackBerry 2FA feature. To use this activation type, you must also assign the BlackBerry 2FA profile to users. When a device is activated, you can view limited device information in the management console, and you can deactivate the device using a command. This activation type is supported only for Microsoft Active Directory users. This activation type is not supported for Apple TV devices. For more information, see the BlackBerry 2FA content.

Activation types: macOS devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls that macOS makes available. When a user activates a macOS device, the device and the user are set up as separate entities on BlackBerry UEM. Separate communication channels are established between BlackBerry UEM and the device and BlackBerry UEM and the user account, allowing you to manage the device and the user separately. Some profiles are assigned to the user only, for example email profiles. Some profiles are assigned to the device only, for example proxy profiles. Some profiles allow you to choose whether to apply the profile to the device or the user, for example Wi-Fi profiles. You can control the device using commands and IT policies. Users activate macOS devices using BlackBerry UEM Self-Service.

Activation types: Android devices

For Android devices, you can select multiple activation types and rank them to make sure that BlackBerry UEM assigns the most appropriate activation type for the device. For example, if you rank "Work and personal - user privacy (Samsung Knox)" first and "Work and personal - user privacy (Android Enterprise)" second, devices that support Samsung Knox Workspace receive the first activation type and devices that don't receive the second.

The Android activation types are organized in the following tables:

- Android Enterprise devices
- Android devices without a work profile
- Samsung Knox Workspace devices

Android Enterprise devices

The following activation types apply only to Android Enterprise devices.

Activation type	Description
Work and personal - user privacy (Android Enterprise with work profile)	This activation type maintains privacy for personal data but lets you manage work data using commands and IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication. To allow Google Play app management for Android Enterprise devices, select **Add Google Play to the workspace**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process. To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** option. Users do not have to grant Administrator permissions to the BlackBerry UEM Client.
Work and personal - full control (Android Enterprise fully managed device with work profile)	This activation type lets you manage the entire device using commands and IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files (if it runs Android 10 or earlier). To allow Google Play app management for Android Enterprise devices, select **Add Google Play account to the work space**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected. Following activation, Work and personal - full control devices have only a limited set of the standard pre-installed apps, such as Camera, Phone, and Settings, in the personal space. The list of retained pre-installed apps depends on the device vendor and OS version. To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** option. To specify whether BlackBerry UEM can limit activation by device ID, select **Allow only approved device IDs**. This activation type requires the device to be reset to factory default settings before activating. If the BlackBerry UEM Client is deleted or the work profile is removed from the device, it is automatically reset to factory default settings. During activation users must grant Administrator permissions to the BlackBerry UEM Client.

Activation type	Description
Work space only (Android Enterprise fully managed device)	This activation type lets you manage the entire device using commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating. The activation process installs a work profile and no personal profile. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password. To allow Google Play app management for Android Enterprise devices, select **Add Google Play to the workspace**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process. During activation, the device installs the BlackBerry UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app. Following activation, Work space only devices have only a limited set of the standard pre-installed apps, such as Camera, Phone, and Settings, plus any apps you have assigned with a required disposition. The list of retained pre-installed apps depends on the device vendor and OS version. To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** option. To specify whether BlackBerry UEM can limit activation by device ID, select **Allow only approved device IDs**. This activation type requires the device to be reset to factory default settings before activating. If the BlackBerry UEM Client is deleted or the work profile is removed from the device, it is automatically reset to factory default settings.

Android devices without a work profile

The following activation types apply to all Android devices.

Activation type	Description
MDM controls	This activation type lets you manage the device using commands and IT policy rules. A separate work space is not created on the device, and there is no added security for work data. **Note:** This activation type is deprecated for devices with Android 10. Attempts to activate Android 10 and later devices with the MDM controls activation type will fail. For more information, visit https://support.blackberry.com/community to read article 48386. If the device supports Knox MDM, this activation type applies the Knox MDM IT policy rules. If you do not want to apply Knox MDM policy rules, clear the **Activate Samsung KNOX on Samsung devices that have the MDM controls activation type assigned** check box. During activation, users must grant Administrator permissions to the BlackBerry UEM Client.
User privacy	You can use the User privacy activation type to provide basic control of devices, including work app management, while making sure that users' personal data remains private. With this activation type, no separate container is installed on the device. To provide security for work data you can install BlackBerry Dynamics apps. Devices activated with User privacy can use services such as Find my Phone and Root Detection, but administrators cannot control device policies. You can also use the User privacy activation type to activate Chrome OS devices to allow you to install and manage Android BlackBerry Dynamics apps.
Device registration for BlackBerry 2FA only	This activation type supports the BlackBerry 2FA solution for devices that BlackBerry UEM does not manage. This activation type does not provide any device management or controls, but allows devices to use the BlackBerry 2FA feature. To use this activation type, you must also assign the BlackBerry 2FA profile to users. When a device is activated, you can view limited device information in the management console, and you can deactivate the device using a command. This activation type is supported only for Microsoft Active Directory users. For more information, see the BlackBerry 2FA content.

Samsung Knox Workspace devices

The following activation types apply only to Samsung devices that support Knox Workspace.

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.

Activation type	Description
Work and personal - user privacy - (Samsung Knox)	This activation type maintains privacy for personal data, but lets you manage work data using commands and IT policy rules. This activation type does not support the Knox MDM IT policy rules. This activation type creates a separate work space on the device and the user must create a password to access the work space. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. The user must also create a Screen lock password to protect the entire device and will not be able to use USB debugging mode. During activation, users must grant Administrator permissions to the BlackBerry UEM Client.
Work and personal - full control (Samsung Knox)	This activation type lets you manage the entire device using commands and the Knox MDM and Knox Workspace IT policy rules. This activation type creates a separate work space on the device and the user must create a password to access the work space. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files (if it runs Android 11 or earlier). During activation users must grant Administrator permissions to the BlackBerry UEM Client.
Work space only - (Samsung Knox)	This activation type lets you manage the entire device using commands and the Knox MDM and Knox Workspace IT policy rules. This activation type removes the personal space and installs a work space. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files. During activation, users must grant Administrator permissions to the BlackBerry UEM Client.

Activation types: Windows 10 devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by Windows 10 devices. A separate work space is not installed on the device and there is no added security for work data. **Note:** Windows 10 Mobile devices are no longer supported by Microsoft. You can control the device using commands and IT policies. Windows 10 users activate devices through the Windows 10 Work access app.

Steps to activate devices

When you set up BlackBerry UEM to allow users to activate devices, you perform the following actions.

Step	Action
1	Verify that all activation requirements are met.
2	Configure the default activation settings.
3	If applicable, review the following information: • If you plan to support Android Enterprise devices, see Supporting Android Enterprise activations. • If you plan to support Windows 10 devices, see Supporting Windows 10 activations. • If you plan to support Apple User Enrollment devices, see Supporting Apple User Enrollment for iOS and iPadOS devices. • If you plan to use zero-touch enrollment for Android Enterprise, Knox Mobile Enrollment, Apple DEP, or Apple Configurator 2 to activate devices, review the related documentation.
4	Update the template for the activation email.
5	Create an activation profile and assign it to user accounts or user groups.
6	Set an activation password for users.

Requirements: Activation

For all devices:

- An available license in BlackBerry UEM for the device that you want to activate.
- A working wireless connection

For iOS, iPadOS, and Android devices:

- The latest version of the BlackBerry UEM Client app installed on the device

For Windows 10 devices:

- A BlackBerry Enterprise Server Root RSA certificate installed on the device
- For devices that use a proxy configuration, a proxy that does not require authentication. For more information, see https://docs.microsoft.com/en-us/windows/client-management/mdm/new-in-windows-mdm-enrollment-management
- Windows 10 Home has only limited support.

Note: Users can watch a video on how to activate their devices.

Turn on user registration with the BlackBerry Infrastructure

Registration with the BlackBerry Infrastructure simplifies the way users activate their mobile devices. With registration turned on, users do not need to enter the server address when they activate devices. Registration is enabled by default. If you change this setting, you might need to update the activation email with the steps that users must take to activate their devices.

Devices running Windows 10 do not use the same method for contacting the BlackBerry Infrastructure, so turning user registration on or off does not change the activation process for these devices. For more information on simplifying the Windows 10 activation process, see the on-prem Configuration content or the Cloud configuration content.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Activation defaults**.
4. Make sure the **Turn on registration with the BlackBerry Infrastructure** check box is selected.
5. Click **Save**.

Managing activation settings

You can manage how users activate devices, including whether users need an activation password or if they can scan a QR Code, how long an activation password or QR Code is valid, and whether users can activate multiple devices with the same password or QR Code.

The following are examples of how you can manage activation settings:

- When you set activation passwords for users, you can do the following:
  - Have BlackBerry UEM autogenerate an activation password or specify an activation password manually.
  - Specify how long the activation password is valid (in minutes or days).
  - Specify that the activation period expires as soon as the user activates a device, effectively limiting the number of devices that a user can activate with that password to one.

  For more information, see Set an activation password and send an activation email message.
- You can include the activation password in a QR Code so that users only need to scan the QR Code in the activation email rather than type the password. For Android Enterprise devices that users will activate with the Work space only or Work and personal - full control activation types, the QR Code can also contain the location to download the BlackBerry UEM Client.
- You can create multiple passwords for a user and pair the passwords with specific activation profiles. For more information, see Allowing users to activate multiple devices with different activation types.
- If you allow users to set activation passwords in BlackBerry UEM Self-Service, users can create activation passwords whenever needed, but they can activate only the number of devices that are specified in the the activation profile. For more information, see Allow users to set activation passwords in BlackBerry UEM Self-Service.
- You can force expiry of an activation password for a user at any time. For more information, see Force activation password expiry.
- If you are deploying devices using Samsung Knox Mobile Enrollment, you can allow users of those devices to use their Microsoft Active Directory credentials to activate their devices. Instead of managing activation passwords for each user, you can instruct users to use their Active Directory credentials. This option applies only to on-premises environments and to devices that are enrolled in your organization's Knox Mobile Enrollment account. For more information, see Specify the default activation settings.

Specify the default activation settings

You can specify the default settings for device activation, including the default time an activation password remains valid before it expires, the length of automatically generated passwords that are sent to users, whether QR Codes can be used for activation, and other options.

For more information on the device activation default settings, see Default device activation settings.

1. On the menu bar, click **Settings > General settings**.
2. Click **Activation defaults**.
3. Under **Device activation defaults** specify activation password and QR Code options.
4. If you are managing Android 9.0 and earlier devices and want to use the MDM controls activation type, select the **Enable MDM controls activation type for Android devices** check box to add MDM controls to the list of activation types in the activation profile.

   This option is enabled by default if BlackBerry UEM has been upgraded from a previous version. If this option is enabled, you can't disable it.

5. Select **Use QR codes to unlock BlackBerry Dynamics apps** to allow users to activate BlackBerry Dynamics apps with a QR Code. For more information, see Generate access keys, activation passwords, or QR Codes for BlackBerry Dynamics apps
6. Select or clear the **Turn on registration with the BlackBerry Infrastructure** check box to modify how users activate their mobile devices. If you don't select this option, users will be asked to provide the server address for BlackBerry UEM when they activate devices. For more information, see Turn on user registration with the BlackBerry Infrastructure.
7. To import or export a list of approved device IDs, browse to your organization's .csv file that contains a list of approved device IDs. For more information see Import or export a list of approved device IDs.
8. Click **Save**.

Default device activation settings

Setting	Description
Activation period expiration	This setting specifies the default length of time that an activation password or QR Code remains valid before it expires. The time can be from 1 minute to 30 days.
Activation period expires after the first device is activated	This setting specifies whether the activation password or QR Code expires after it is used to activate a device.
Allow QR Codes for device activation	This setting specifies whether a QR Code can be included in the activation email message and displayed in BlackBerry UEM Self-Service. Users can scan the QR Code to initiate device activation. If this option is not selected, the option to send a QR Code is not available for the activation email template.
Allow QR Code to contain activation password	This setting specifies whether the QR Code contains the activation password. If this option is selected, users don't need to separately type a password after scanning a QR code to activate a device.
Allow QR Code to contain location of UEM Client app source file	This setting specifies whether the QR Code code contains a location for the device to download the UEM Client app source (.apk) file. This setting is relevant only for activating Android Enterprise devices with the Work space only and Work and personal - full control activation types. Scanning the QR Code with the device initiates downloading and installing the BlackBerry UEM Client .
Use default location	If you allow the QR Code to contain the location of the UEM Client source file, select this option to specify that the device should get the .apk file from the BlackBerry download site.
Location of UEM Client app source file	If you allow the QR Code to contain the location of the UEM Client source file, this setting specifies the location that the device downloads the file from. You can specify any location that the device has access to when it is set to factory default settings.
Allow use of Microsoft Active Directory username and password	For devices that are activated using Samsung Knox Mobile Enrollment, this setting specifies whether to allow users to use their Microsoft Active Directory credentials to activate devices.
Send device activated notification	This setting specifies whether the user receives an email message when a device is activated.

Setting	Description
Autogenerated activation password length	This setting specifies the number of characters in an automatically generated password. The value can be from 4 to 16.
Autogenerated password complexity	This setting specifies the types of characters in an automatically generated password. Passwords can include the following types of characters: • Lowercase letters • Uppercase letters • Numbers • Special characters or symbols
Enable MDM controls activation type for Android devices	This setting specifies whether MDM controls is included in the list of Android activation types in the activation profile. Google has deprecated this activation type for devices with Android 10 and later. For more information, visit https://support.blackberry.com/community to read article 48386. This option is enabled by default if BlackBerry UEM has been upgraded from a previous version. If this option is enabled, you can't disable it.
Use QR codes to unlock BlackBerry Dynamics apps	This setting specifies whether users can activate BlackBerry Dynamics apps with a QR Code. For more information, see Generate access keys, activation passwords, or QR Codes for BlackBerry Dynamics apps.
Turn on registration with the BlackBerry Infrastructure	This setting specifies Select or clear the **Turn on registration with the BlackBerry Infrastructure** check box to modify how users activate iOS, iPadOS, macOS, and Android devices. If you deselect this option, users will be asked to provide the server address for BlackBerry UEM when they activate devices. For more information, see Turn on user registration with the BlackBerry Infrastructure.

Allowing users to activate multiple devices with different activation types

You can create multiple activation passwords for a user and pair the activation passwords with specific activation profiles so that users can activate devices with different activation types.

For example, you might want users to activate work devices with an activation type that allows you to have full control of devices, but activate their personal devices with an activation type that allows user privacy. By pairing one activation password with an activation profile that allows full device control and a second activation password with the user privacy activation profile, users can activate each device with different results. You can create email templates that describe the intended use for each password.

Select the "Device activation with specified activation profile" option when you create a user account or send an activation email message.

At a given time, you can have a maximum of two activation passwords that are paired with specific activation profiles. Each password can be used to activate multiple devices.

Note: For activation passwords that are paired with specific activation profiles, the "Number of devices that a user can activate" setting in the activation profile is not enforced.

If you delete an activation profile that an activation password is paired with, the activation password is automatically expired.

If necessary, you can expire activation passwords for a particular user at any time. For more information, see Force activation password expiry.

Unlike regular activation passwords, users cannot create activation passwords that are paired with specific activation profiles in BlackBerry UEM Self-Service.

This option is not supported by iOS devices that are enrolled in DEP.

Force activation password expiry

You can manually force an activation password that was generated for a user to expire.

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. In the **Activation details** section, locate the activation password that you want to expire. Click **Expire**. The activation password is expires immediately.

   If you force a regular activation password to expire, the date and time that the password expired is displayed.

   If you force an activation password that was paired with a specific activation profile to expire, the details of the device activation password are no longer displayed.

Set an activation password and send an activation email message

You can set an activation password and send a user an activation email with the information required to activate one or more devices.

In on-premises environments, the email message is sent from the email address that you configured in the SMTP server settings.

Before you begin: Create an activation email template.

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. In the Activation details pane, click **Set activation password**.
5. In the **Activation option** drop-down list, perform one of the following tasks:
   - If you want the user to activate their device with the activation profile that is currently assigned to them, select **Default device activation**. You can see the activation profile that is assigned to the user in the IT policy and profiles section on the Summary tab.
   - If you want to pair an activation password with a specific activation profile, select **Device activation with specified activation profile**. For more information, see Allowing users to activate multiple devices with different activation types.
6. In the **Activation password** drop-down list, perform one of the following tasks:
   - If you want to automatically generate a password, select **Autogenerate device activation password and send email with activation instructions**. When you select this option, you must select an email template to send the information to the user.

- If you want to set an activation password for the user and, optionally, send an activation email, select **Set device activation password**.

7. Optionally, change the activation period expiration. The activation period expiration specifies how long the activation password remains valid.
8. If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**.
9. In the **Activation email template** drop-down list, select the email template that you want to use.
10. Click **Submit**.

Send an activation email to multiple users

You can send activation email messages to multiple users at one time. When you send an activation email to multiple users, the activation password is autogenerated. If you want to set the activation password, see Set an activation password and send an activation email message.

The email is sent from the email address that you configured in the SMTP server settings.

Before you begin: Create an activation email template.

1. On the menu bar, click **Users > Managed devices**.
2. Select the check box for each user that you want to send an activation email to.
3. Click  .
4. In the **Activation option** drop-down list, perform one of the following tasks:
   - If you want users to activate their devices with the activation profile that is currently assigned to them, select **Default device activation**.
   - If you want to pair an activation password with a specific activation profile, select **Device activation with specified activation profile**. For more information about pairing activation passwords with activation profiles, see Allowing users to activate multiple devices with different activation types.
5. In the **Activation password** drop-down list, select **Autogenerate device activation password and send email with activation instructions**.
6. Optionally, change the activation period expiration. The activation period expiration specifies how long the activation password remains valid.
7. If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**.
8. In the **Activation email template** drop-down list, select the email template that you want to use.
9. Click **Send**.

Allow users to set activation passwords in BlackBerry UEM Self-Service

You can allow users with iOS, Android, and Windows devices to create their own activation passwords using BlackBerry UEM Self-Service.

1. On the menu bar, click **Settings > Self-Service > Self-Service settings**.
2. Select **Allow users to activate devices in the self-service console** and complete the following tasks:
   a) Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires.

b) Specify the minimum number of characters required in an activation password.
c) In the **Minimum password complexity** drop-down list, select the level of complexity required for activation passwords.
d) To automatically send an activation email to users when they create an activation password, select the **Send activation email** check box and select an email template from the **Activation email template** drop-down list.
e) To send custom activation messages to users, select the **Send custom activation messages** check box. Select a message template for each device type from the appropriate drop-down list.
f) To send login notification emails to users each time they log in to BlackBerry UEM Self-Service, select the **Send self-service login notification** check box.

3. Click **Save**.

Supporting Android Enterprise activations

How users activate Android Enterprise devices can depend on several factors, including the Android OS version, how much control your organization wants to have over user's devices, and how your organization uses Google services. Your organization may interact with Google services in the following ways:

Google services connection	Description
Managed Google Play accounts	BlackBerry UEM is not connected to a Google domain. You can use managed Google Play accounts to allow users to download and install work apps using Google Play. For more information, see Support Android Enterprise activations using managed Google Play accounts
Google Workspace domain	Your organization has a Google Workspace domain, which supports all Google Workspace services such as Gmail, Google Calendar, and Google Drive. For more information, see Support Android Enterprise activations with a Google Workspace domain
Google Cloud domain	Your organization has a Google Cloud domain, which provides managed Google accounts to users. Your organization doesn't use Google Workspace services such as Gmail, Google Calendar, and Google Drive for your organization's email, calendar, and data management. For more information, see Support Android Enterprise activations with a Google Cloud domain
No Google services	Your organization's security policies do not allow you to use Google services. For more information, see Support Android Enterprise devices without access to Google Play

For more information on configuring BlackBerry UEM to connect to a Google domain or use managed Google Play accounts, see the on-premises Configuration content or the Cloud Configuration content.

Support Android Enterprise activations using managed Google Play accounts

If your organization doesn't have a Google domain or you don't want to connect BlackBerry UEM to your Google domain, you can activate Android Enterprise devices to use managed Google Play accounts. Managed Google Play accounts allow you to add internal apps to Google Play that only your users activated devices can download. For more information about managed Google Play accounts, see https://support.google.com/googleplay/work/.

To use managed Google Play accounts with BlackBerry UEM, you use any Google or Gmail account to connect BlackBerry UEM to Google. No personally identifiable information about your users is sent to Google After you connect BlackBerry UEM to Google, you can allow users to activate Android Enterprise devices and download work apps using Google Play. For information about configuring BlackBerry UEM to support Android Enterprise devices, see the on-premises Configuration content or the UEM Cloud Configuration content.

Support Android Enterprise activations with a Google Workspace domain

If you have configured BlackBerry UEM to connect to a Google Workspace domain, you must perform the following tasks before users can activate Android Enterprise devices.

Before you begin: Configure BlackBerry UEM to support Android Enterprise devices. For information about configuring BlackBerry UEM to support Android Enterprise devices, see the on-premises Configuration content or the UEM Cloud Configuration content.

1. In your Google Workspace domain, create user accounts for your Android users.
2. Select the **Enforce EMM Policy** setting in the Google Workspace domain.

   This setting is required for devices with the Work space only and Work and personal - full control activation types and strongly recommended for devices with other activation types. If this setting is not selected, users can add a managed Google account to the device that can access work apps outside of the work profile.
3. If you intend to assign the Work space only or Work and personal - full control activation type, select the **Enforce EMM Policy** setting in the Google Workspace domain.
4. In BlackBerry UEM, create local user accounts for your Android users. Each account's email address must match the email address in the corresponding Google Workspace account.
5. Make sure that your users know the passwords for their Google Workspace accounts.
6. In BlackBerry UEM, assign an email profile and productivity apps to users, user groups, or device groups.

Support Android Enterprise activations with a Google Cloud domain

If you have configured BlackBerry UEM to connect to a Google Cloud domain, you must perform the following tasks before users can activate devices using Android Enterprise.

Before you begin: Configure BlackBerry UEM to support Android Enterprise. When you configure BlackBerry UEM to connect to a Google Cloud domain, you must select whether BlackBerry UEM can create user accounts in the domain. This selection affects the tasks that you must perform before users can activate Android Enterprise devices. For information about configuring BlackBerry UEM to support Android Enterprise devices, see the on-premises Configuration content or the UEM Cloud Configuration content.

1. In BlackBerry UEM, add directory user accounts for your Android Enterprise users.
2. If you choose not to allow BlackBerry UEM to create user accounts in your Google Cloud domain, you must create user accounts in your Google Cloud domain and in BlackBerry UEM. Perform one of the following actions:

   - In your Google Cloud domain, create user accounts for your Android Enterprise users. Each email address must match the email address in the corresponding BlackBerry UEM user account. Make sure that your Android Enterprise users know the password for their Google Cloud accounts.
   - Use the Google Apps Directory Sync tool to synchronize your Google Cloud domain with your company directory. If you do this, you don't need to create user accounts manually in your Google Cloud domain.
3. If you intend to assign the Work space only or Work and personal - full control activation types, select the **Enforce EMM Policy** setting in the Google Cloud domain.

   This setting is required for devices with the Work space only and Work and personal - full control activation types and strongly recommended for devices with other activation types. If this setting is not selected, users can add a managed Google account to the device that can access work apps outside of the work profile.
4. In BlackBerry UEM, assign an email profile and productivity apps to users, user groups, or device groups.

Support Android Enterprise devices without access to Google Play

To activate devices that don't have access to Google Play, users must download the latest BlackBerry UEM Client from a different source. The available methods to download the UEM Client depend on the OS version and activation type:

- For devices that will be activated with the Work space only or Work and personal - full control activation types, the device must be set to factory default settings before installing the UEM Client. To provide the download location to the device, you can include the location in a QR Code that the user scans to start activation, or allow the device to get download information using NFC (for example, by tapping an NFC sticker or another device).
  - For information on including the UEM Client location in a QR Code, see Default device activation settings.
  - For information on programming an NFC sticker, see Program an NFC sticker to activate devices.
  - For information on using the BlackBerry UEM Enroll app on a secondary device to provide UEM Client download instructions over NFC, see the UEM Enroll documentation. To use this method, the BlackBerry UEM Enroll app must be installed on an Android 9 device and the device to be activated must have Android 9 or earlier.
- Devices that will be activated with the Work and personal - user privacy activation type, don't need to be reset to factory default settings first. For these devices, users can download the BlackBerry UEM Client from the BlackBerry download site or another available location after the out-of-box device setup is complete.

To download the .apk file of the latest UEM Client or UEM Enroll app, visit support.blackberry.com/community to read article 42607.

For instructions to activate Android Enterprise devices, see Activating Android devices

Requirements

If you want to activate devices that don't have access to Google Play, verify the following:

Requirement	Description
BlackBerry UEM environment	• **Integration with Android Enterprise**: You are not required to integrate UEM with Android Enterprise if you want to support only devices that don't have access to Google Play. If you want to support a mix of devices that do and don't have access to Google Play, you must integrate the UEM environment with Android Enterprise.
Device activation default settings	If you want to include the UEM Client location in a QR code, verify the following device activation default settings: • Select the **Allow QR code to contain location of UEM Client app source file** and **Use default location** options. These options allow users to scan the QR code in the activation email to download the UEM Client from the BlackBerry download site. These options are available only if your UEM environment is integrated with Android Enterprise.

Requirement	Description
Activation profile settings	Verify the following settings in the activation profile: • Deselect the **Add Google Play account to workspace** option. This option is available only if your UEM environment is integrated with Android Enterprise. • If you want to enable BlackBerry Secure Connect Plus, select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** option. You must upload the BlackBerry Connectivity app as an internal app and assign it to users.
IT policy rules	For users that are assigned the Work and personal - user privacy (Android Enterprise) activation type, verify the following in the IT policy: • Enable the **Allow installation of non Google Play apps** IT policy rule to allow the installation of apps outside of Google Play.
Non- BlackBerry Dynamics apps	For non-BlackBerry Dynamics apps, add the apps to UEM as internal apps and assign them to users. **1.** Obtain the .apk files of the apps that you want to assign. For example, to download the latest version of the BlackBerry Connectivity app, visit the BlackBerry myAccount portal. **2.** In the BlackBerry UEM management console, on the menu bar, click **Apps**. **3.** Click > **Internal apps**. **4.** Click **Browse** and select the .apk file. **5.** In the **Send to** field, select **All Android devices**. **6.** Deselect **Publish app in Google domain**. **7.** Click **Add**. **8.** Repeat the previous steps for each app that you want to add. **9.** Assign the apps to users. The app disposition must be set to **Required**.
BlackBerry Dynamics apps	For BlackBerry Dynamics apps, upload the internal app source file and assign the app to users. Perform the following steps to install or update internal apps on devices that don't have access to Google Play: **1.** Obtain the .apk files of the BlackBerry Dynamics apps that you want to assign. For example, to download BlackBerry Work, visit support.blackberry.com/community and read article 42607. **2.** In the BlackBerry UEM management console, on the menu bar, click **Apps**. **3.** Click a BlackBerry Dynamics app (for example, BlackBerry Work). **4.** Click the **Android** tab. **5.** Click **Add internal app source file**. **6.** Click **Browse** and select the .apk file. **7.** Click **Add**. **8.** Click **Save**. **9.** Repeat the previous steps for each app that you want to add. **10.** Assign the apps to users. The app disposition must be set to **Required**.

Requirement	Description
BlackBerry UEM Client app update	To update the UEM Client app on devices, users must manually download the latest version of the .apk file and install it. For more information, visit support.blackberry.com/community and read article 42607.

For more information about supporting Android Enterprise devices without access to Google Play, visit support.blackberry.com/community to read article 57492.

Program an NFC sticker to activate devices

Users can download the BlackBerry UEM Client and initiate device activation by tapping the device on an NFC tag or sticker. This method is one option to activate Work space only (Android Enterprise) and Work and personal - full control (Android Enterprise) devices that don't have access to Google Play.

To allow users to activate devices using this method, you program a third-party NFC sticker with the values needed to instruct the device to download the UEM Client and begin activation.

Before you begin: You need the following items:

- NFC tag or sticker
- A method to program the sticker such as an Android app that can read and write to NFC stickers.

1. In the management console, click **Settings > External integration > Android Enterprise**.
2. Under **NFC enrollment**, click **Learn more**.
3. On a device with an app that can write data to NFC stickers, open the app and allow the app to connect to the sticker that you want to program and add the following settings:
   a) Set the NFC data type to `custom`.
   b) Set the content type to `application/com.android.managedprovisioning`
   c) Copy the details from the text box in the management console to the **Configuration** field in the app.
4. Write the settings to the sticker.

After the program is written to the sticker, users should be able to tap the sticker with a new device or a device reset to factory settings to download the UEM Client and start the activation.

Supporting Windows 10 activations

You can help users activate Windows 10 devices in the following ways:

- Create or edit an activation email template to provide Windows 10 activation information. For more information, see "Create an activation email template."
- **Integrate BlackBerry UEM with Azure Active Directory join**: When Azure Active Directory join is configured, users can activate their devices using only their Azure Active Directory username and password. An Azure Active Directory premium license is required. For more information, see the on-prem Configuration content or the Cloud configuration content.
- **Configure Windows Autopilot**: When you configure Windows Autopilot, the enrollment is part of the out-of-box setup experience and the device is automatically activated when the user completes it using only their Azure Active Directory username and password. Integration with Azure Active Directory join and an Azure Active Directory premium license are required. For more information about Windows Autopilot, visit the Microsoft website.
- **Deploy a discovery service**: You can use a Java web application from BlackBerry as a discovery service. You can use different operating systems and web application tools to deploy a discovery service web application. For more information, see the on-prem Configuration content or the Cloud configuration content.

Supporting Apple User Enrollment for iOS and iPadOS devices

You can use the User privacy - User enrollment activation type for iOS and iPadOS devices to make sure that user data is kept private and separated from work data. With this activation type, a separate work space is installed on the device for work apps and the native Notes, iCloud Drive, Mail (attachments and full email bodies), Calendar (attachments), and iCloud Keychain apps. This activation type enables app management, IT policy management, email profiles, Wi-Fi profiles, and per-app VPN. Administrators can manage work data (for example, wipe work data) without affecting personal data. This activation type is supported on unsupervised iPhone and iPad devices that run iOS or iPadOS 13.1 or later.

If you want to support Apple User Enrollment, verify the following:

- Verify that the devices that you will activate using this activation type are not supervised.
- Create a managed Apple ID account for each user. The managed Apple ID email address must match the user's email address in BlackBerry UEM.
- When you set the device activation password for a user, make sure to select the Apple User Enrollment activation email template.
- Assign the BlackBerry UEM Client using a VPP license to users if you want to allow them to easily activate other BlackBerry Dynamics apps, import certificates, use BlackBerry 2FA features, use CylancePROTECT, and check their compliance status. If you set the disposition to Required, the user is prompted to install the app. If you set the disposition to Optional, the user must manually download the app from Work Apps.

Supporting Samsung Knox DualDAR

Devices that support Samsung Knox DualDAR encryption can have work data secured using two layers of encryption. The outer layer of Knox DualDAR is built on Android file-based encryption and enhanced by Samsung to meet MDFPP requirements. In the activation profile, you can specify whether to use the default built-in encryption app or an internal encryption app that you want to use for the inner layer of encryption in the work profile. If you choose to use the default app, the work profile is secured using a FIPS 140-2 certified cryptographic module that is included in the Samsung Knox framework. The internal encryption app is a purpose-built cryptographic module that is developed by your organization or a third party and is expected to be FIPS 140-2 certified. When the user is not using the device, all data in the work profile is locked and can't be accessed by apps running in the background.

Requirement	Description
Supported devices	Samsung Galaxy S10, Samsung Galaxy Note 10, and future Samsung flagship models
Encryption app	If you have an encryption app that you want to use for Knox DualDAR encryption, you must add it as an internal app in the BlackBerry UEM management console. You select this encryption app when you create an activation profile for devices that support Knox DualDAR. You can also choose to use the default encryption app instead.
Activation profile	To support Knox DualDAR encryption, create an activation profile with the following settings for Android devices: • Select the Work and personal - full control (Android Enterprise fully managed device with work profile) activation type • Select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** option. • Select the **Enable Samsung Knox DualDAR Workspace** option. • To use the default encryption app, select the **Default built-in encryption app** option. To use another encryption app, select the **Select an internal app for encryption** option and choose the encryption app that you want from the app list. **Note:** If you enable Knox DualDAR encryption in the activation profile, you should assign the profile to devices that support it only. If your organization supports a mix of devices that may or may not support Knox DualDAR, you should assign the activation profile to a device group. If you enable KnoxDualDAR activation for an unsupported device, the activation will not complete successfully.
BlackBerry UEM Client	A version of BlackBerry UEM Client for Android later than 12.35.2.155980 is required.

Enable user notification when a device has been activated

You can enable UEM to notify a user each time a device is activated on their account. The email notification is sent to the email address of the user account that was used to activate the device. By default, the email includes the device model, serial number, and IMEI. If the user receives a notification that they were not expecting, they should contact an administrator.

1. On the menu bar, click **Settings** > **General settings**.
2. Click **Activation Defaults**.
3. Select **Send device activated notification**.
4. Click **Save**.

Creating activation profiles

You can control how devices are activated and managed using activation profiles. An activation profile specifies how many and what types of devices a user can activate and the type of activation to use for each device type.

The activation type allows you to configure how much control you have over activated devices. You might want complete control over a device that you issue to a user. You might want to make sure that you have no control over the personal data on a device that a user owns and brings to work.

The assigned activation profile applies only to devices the user activates after you assign the profile. Devices that are already activated are not automatically updated to match the new or updated activation profile.

When you add a user to BlackBerry UEM, the Default activation profile is assigned to the user account. You can change the Default activation profile to suit your requirements, or you can create a custom activation profile and assign it to users or user groups.

Create an activation profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > Activation**.
3. Click +.
4. Type a name and description for the profile.
5. In the **Number of devices that a user can activate** field, specify the maximum number of devices the user can activate.
6. In the **Device ownership** drop-down list, select the default setting for device ownership.
   - Select **Not specified** if some users activate personal devices and some users activate work devices.
   - Select **Work** if most users activate work devices.
   - Select **Personal** if most users activate their personal devices.
7. Optionally, select an organization notice in the **Assign organization notice** drop-down list. If you assign an organization notice, users activating iOS, iPadOS, macOS, or Windows 10 devices must accept the notice to complete the activation process.
8. In the **Device types that users can activate** section, select the device OS types that users can activate. Device types that you don't select are not included in the activation profile and users can't activate those devices.
9. Perform the following actions for each device type included in the activation profile:
   a) Click the tab for the device type.
   b) In the **Device model restrictions** drop-down list, select one of the following options:
      - **No restrictions**: Users can activate any device model.
      - **Allow selected device models**: Users can activate only the device models that you specify. Use this option to limit the allowed devices to only some models.
      - **Do not allow selected device models**: Users can't activate the device models that you specify. Use this option to block activation of some device models or devices from specific manufacturers.

      If you restrict the device models users can activate, click **Edit** to select the devices you want to allow or restrict and click **Save**.
   c) In the **Minimum allowed version** drop-down list, select the minimum allowed OS version.

      Many older OS versions are no longer supported by BlackBerry UEM. You only need to select a minimum version if you don't want to support the earliest version currently supported by BlackBerry UEM. For more information on supported versions, see the Compatability Matrix.

d) Select the supported activation types.

   For Android devices, you can select multiple activation types and rank them. For all other device types, you can select only one activation type.

   The "MDM controls" activation type is deprecated for devices with Android 10 and later. It is included in the list of activation types only if the **Enable MDM controls activation type for Android devices** setting is selected in the default activation settings.

10. For iOS and iPadOS devices, perform the following actions:

a) If you selected the "User privacy" activation type and you want to enable SIM-based licensing, select **Allow access to SIM card and device hardware information to enable SIM-based licensing**.

b) If you selected the "User privacy" activation type and you want to manage specific features, select the appropriate check boxes. For more information on each option, see Activation types: iOS devices.

c) If you selected the "MDM controls" or "User privacy" (with SIM-based licensing) activation types and you only want to activate supervised devices, select **Do not allow unsupervised devices to activate**

d) In the **iOS app integrity check** section, optionally select one of the following attestation methods:

- **Perform app integrity check on BlackBerry Dynamics app activation**: Use this method to send challenges to devices when they are activated to check the integrity of iOS work apps.
- **Perform periodic app integrity checks**: Use this method to send challenges to devices to check the integrity of iOS work apps.

To perform iOS app integrity checking, you must enable CylancePROTECT in your BlackBerry UEM domain. For more information, see the BlackBerry Protect Mobile content.

11. For Android devices, perform the following actions:

a) If you selected more than one activation type type, click the up and down arrows to rank them.

Devices receive the highest ranked profile that they support. For example, if you rank "MDM Controls" first, devices that don't support "MDM Controls" receive the next ranked activation type.

b) If you selected the "MDM controls" activation type and you don't want Knox MDM policy rules to be applied to the devices that support them, clear the **Activate Samsung KNOX APIs on MDM Controls activations** check box.

c) If you selected a Samsung Knox activation type and you want to use Google Play to manage work apps, select **Google Play app management for Samsung Knox Workspace devices**. This option is available only if you have configured a connection to a Google domain.

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.

d) If you selected an Android Enterprise activation type, enable the appropriate Android Enterprise options:

- **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** enables BlackBerry Secure Connect Plus and Knox Platform for Enterprise features (for devices that support Samsung Knox) on devices with an appropriate license.
- **Enable Samsung Knox DualDAR Workspace** enables Samsung Knox DualDAR encryption for devices that support it. This option is supported only by "Work space only" and "Work and personal - full control" devices.
- **Add Google Play account to work space** allows Google Play app management in the work space. If the device does not have access to Google Play, deselect this option.
- **Allow only approved device IDs** allows you to restrict activation to individual devices that you specify the device ID for. This option is supported only for "Work space only" and "Work and personal - full control" devices.
- **Zero Touch QR Code enrollment** allows you specify whether users can activate a device using a QR Code over a Wi-Fi or mobile network. The default setting is Wi-Fi. Users can activate using only the

network type that you specify. This option is supported only for "Work space only" and "Work and personal - full control" devices.

e) In the **SafetyNet or Play Integrity attestation options** section, optionally select one of the following attestation methods:

- **Perform SafetyNet or Play Integrity attestation for device**: Use this method to send challenges to test the authenticity and integrity of devices.
- **Perform SafetyNet or Play Integrity attestation on device activation**: Use this method to send challenges to test the authenticity and integrity of devices when they are activated.
- **Perform SafetyNet or Play Integrity attestation on BlackBerry Dynamics app activation**: Use this method to send challenges to test the authenticity and integrity of BlackBerry Dynamics apps when they are activated.

f) In the **Hardware attestation options** section, select **Enforce attestation compliance rules during activation** if you want BlackBerry UEM to send challenges to devices when they are activated to ensure the required security patch level is installed.

12. For Windows 10 devices, select one or both form factor options.

Windows 10 Mobile devices are no longer supported by Microsoft and have only limited support in BlackBerry UEM.

13. Click **Add**.

After you finish: If necessary, rank profiles.

Device activation instructions

If necessary, you can provide users with step-by-step instructions to activate devices.

The steps for individual users may differ slightly from those documented here depending on the user's device model and OS version.

Activating Android devices

The steps users follow to install the BlackBerry UEM Client and initiate Android device activation depend on several factors, including the Android OS version, the device manufacturer, how your organization uses Google services, the activation type specified in the device activation profile, and your organization's preferences. You can provide instructions to users in the activation email that BlackBerry UEM sends to users. For more information, see Email templates.

Android Enterprise devices support several methods for users to start the activation process:

Activation method	Description
Install the UEM Client from Google Play	Devices that will be activated with the Work and personal - user privacy activation type don't need to be reset to factory default settings before activation. To activate these devices, users can download the UEM Client to their device from Google Play. For more information, see Activate an Android Enterprise device with the Work and personal - user privacy activation type.
User downloads the UEM Client from the BlackBerry download site	In situations where Android users don't have access to Google Play, for devices that will be activated with the Work and personal - user privacy activation type, users can download the UEM Client .apk file from the BlackBerry download site or you can download the file from BlackBerry and put it in a location that your users can access. For more information, visit support.blackberry.com/community to read article 42607.
Enter Google domain credentials during device setup	If BlackBerry UEM is connected to your organization's Google Workspace or Google Cloud domain, to activate devices that are assigned the Work space only or Work and personal - full control activation type, when users enter their work Google credentials during device setup the device downloads the UEM Client and begins the activation process. For more information, see Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain.

Activation method	Description
Scan a QR Code that contains the UEM Client download location	BlackBerry UEM allows you to include the download location for the UEM Client in the QR Code added to the activation email sent to users. To activate devices that are assigned the Work space only or Work and personal - full control activation type, users can tap the device Start screen seven times to open a QR Code reader and scan the QR Code. Some device manufacturers may not support this functionality. For more information, see Activate an Android Enterprise device with the Work and personal - full control activation type using a managed Google Play account.
Tap an NFC sticker or a secondary device with the BlackBerry UEM Enroll app that is programmed with the UEM Client download location	You can program an NFC sticker or set up a secondary device that has the UEM Enroll app installed. To activate devices that are assigned the Work space only or Work and personal - full control activation type, users can tap the NFC sticker or the secondary device to start the UEM Client download. The same secondary device or NFC sticker can be used to activate devices for multiple users. For more information, see Activate an Android Enterprise device without access to Google Play.
Android zero-touch enrollment or Samsung Knox Mobile Enrollment	Android zero-touch enrollment allows you to deploy a large number of Android Enterprise devices at one time. Knox Mobile Enrollment allows you to deploy large numbers of Samsung Knox devices with Android Enterprise activations. To use these option, devices must be provisioned for zero-touch enrollment or Knox Mobile Enrollment when they are purchased from an authorized reseller. For more information see Configure support for Android zero-touch enrollment or Activate multiple devices using Knox Mobile Enrollment.

Each option to download the UEM Client and start device activation is supported only by certain activation types. For the Work space only and Work and personal - full control activation types, the supported options also depend on how your organization uses Google services.

Activation type	Work and personal - user privacy	Work and personal - full control			Work space only		
Method		Google domain	Managed Google Play	No Google access	Google domain	Managed Google Play	No Google access
Install UEM Client from Google Play or user download	Yes	No	No	No	No	No	No
Google domain credentials	Yes	Yes	No	No	Yes	No	No

Activation type	Work and personal - user privacy	Work and personal - full control			Work space only		
Method		**Google domain**	**Managed Google Play**	**No Google access**	**Google domain**	**Managed Google Play**	**No Google access**
Scan QR Code	No	Yes	Yes	Yes	Yes	Yes	Yes
Tap NFC sticker or secondary device	No	Yes	Yes	Yes	Yes	Yes	Yes
Android zero-touch enrollment / Samsung Knox Mobile Enrollment	No	Yes	Yes	Yes	Yes	Yes	Yes

Activate an Android Enterprise device with the Work and personal - user privacy activation type

These steps apply to activating devices that are assigned the Work and personal - user privacy (Android Enterprise) activation type. Devices with this activation type don't need to be reset to factory default settings before activation.

Send the following activation instructions to the device users, or send them a link to the following workflow: Activate your Android device.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. If the email message includes an activation QR Code, you can use it to activate your device and you don't need to type any information. If you did not receive a QR Code, make sure you received the following information:

- Your work email address
- BlackBerry UEM username (usually your work username)
- BlackBerry UEM activation password
- BlackBerry UEM server address (if required)

1. On the device, install the BlackBerry UEM Client from Google Play.

   If the device doesn't have access to Google Play, you can manually download the UEM Client from BlackBerry and install it. To download the .apk file of the latest UEM Client , visit support.blackberry.com/community to read article 42607.
2. Open the UEM Client.
3. Read the license agreement and tap the **I accept the License Agreement** checkbox.
4. Do one of the following:

Task	Steps
Use a QR Code to activate the device	**a.** Tap . **b.** Tap **Allow** to allow the UEM Client to take pictures and record video. **c.** Scan the QR Code in the activation email message that you received.

Task	Steps
Manually activate the device	**a.** Type your work email address. Tap **Next**. **b.** Type your activation password. Tap **Activate My Device**. **c.** If necessary, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service. Tap **Next**. **d.** If necessary, type your username and activation password. Tap **Next**.

5. Tap **Allow** to allow the UEM Client to make and manage phone calls.
6. Wait while the profiles and settings are pushed to your device.
7. On the **Set up your profile** screen, tap **Set up** and wait while a work profile is set up on the device.
8. If you are prompted, log in to your Google account with your Google email address and password.
9. On the unlock selection screen, choose a screen unlock method.
10. If you are prompted with the **Secure start-up** screen, tap **Yes** to require a password when the device starts.
11. Type a device password and type it again to confirm it. Tap **OK**.
12. Select one of the options for how you want your notifications to show. Tap **Done**.
13. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
14. On the next screen, tap **Enroll** and follow the instructions on the screen if you want to set up fingerprint authentication for the UEM Client and any BlackBerry Dynamics apps that you have. Otherwise, tap **Cancel**.
15. If you are signed out of your device, unlock your device to complete the BlackBerry UEM activation.
16. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
17. If you are prompted, follow the instructions on the screen to install work apps on your device.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- In the UEM Client, tap ⋮ > **About**. In the **Activated Device** section, verify that the device information and the activation time stamp are present.
- In the BlackBerry UEM Self-Service console, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain

These steps apply to devices that are assigned the Work space only (Android Enterprise) or Work and personal - full control (Android Enterprise) activation type when BlackBerry UEM is connected to a Google Workspace or Google Cloud domain. To activate devices that are connected to a Google domain with the Work and personal - user privacy activation type, see Activate an Android Enterprise device with the Work and personal - user privacy activation type.

This topic describes one method to activate Android Enterprise devices. For information about additional options, see Activating Android devices.

Send the following activation instructions to the device user.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. If the email message includes an activation QR Code, you can use it to activate your device and you don't need to type any information. If you did not receive a QR Code, make sure you received the following information:

- Your work email address

- BlackBerry UEM activation username (usually your work username)
- BlackBerry UEM activation password
- BlackBerry UEM server address (if required)

1. If you do not see the device setup Welcome screen, reset your device to the factory default settings.
2. During the device setup, in the Google account login screen, enter your work Google email address and password.
3. On the device, tap **Install** to install the BlackBerry UEM Client.
4. Read the license agreement and tap the **I accept the License Agreement** checkbox.
5. Do one of the following:

Task	Steps
Use a QR Code to activate the device	**a.** Tap . **b.** Tap **Allow** to allow the UEM Client to take pictures and record video. **c.** Scan the QR Code in the activation email message that you received.
Manually activate the device	**a.** Type your work email address. Tap **Next**. **b.** Type your activation password. Tap **Activate My Device**. **c.** If necessary, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service. Tap **Next**. **d.** If necessary, type your username and activation password. Tap **Next**.

6. Wait while the profiles and settings are pushed to your device.
7. On the **Set up your profile** screen, tap **Set up** and wait while a work profile is set up on the device.
8. If you are prompted, log in to your Google account with your Google email address and password.
9. On the unlock selection screen, choose a screen unlock method.
10. If you are prompted with the **Secure start-up** screen, tap **Yes** to require a password when the device starts.
11. Type a device password and type it again to confirm it. Tap **OK**.
12. Select one of the options for how you want your notifications to show. Tap **Done**.
13. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
14. On the next screen, tap **Enroll** and follow the instructions on the screen if you want to set up fingerprint authentication for the UEM Client and any BlackBerry Dynamics apps that you have. Otherwise, tap **Cancel**.
15. If you are signed out of your device, unlock your device to complete the BlackBerry UEM activation.
16. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
17. If you are prompted, follow the instructions on the screen to install work apps on your device.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- In the UEM Client, tap > **About**. In the **Activated Device** section, verify that the device information and the activation time stamp are present.
- In the BlackBerry UEM Self-Service console, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activate an Android Enterprise device with the Work and personal - full control activation type using a managed Google Play account

This topic describes one method to activate Android Enterprise devices. For information about additional options, see Activating Android devices.

For Android 10 devices, the instructions to activate an Android Enterprise device with the Work space only activation type using a managed Google Play account also work for the Work and personal - full control activation type. Android 11 no longer supports using the afw#blackberry hashtag to initiate Work and personal - full control activations.

These instructions use the QR Code to instruct the device to download and install the BlackBerry UEM Client. To allow users to initiate the download with the QR Code, in the default activation settings, you must select **Allow QR Code to contain location of UEM Client app source file**. For more information, see Specify the default activation settings.

Send the following activation instructions to the device user.

Before you begin: Your device administrator sent you one or more email messages with the information that you need to activate your device. The email message includes a QR Code with the information needed to install the UEM Client and activate the device.

1. On the device that you want to activate, if you don't see the first device setup screen, reset your device to the factory default settings.
2. Tap the device screen seven times.

   A QR Code reader opens on the device.
3. Read the license agreement and tap the **I accept the License Agreement** checkbox.
4. Wait while the profiles and settings are pushed to your device.
5. On the **Set up your profile** screen, tap **Set up** and wait while a work profile is set up on the device.
6. If you are prompted, log in to your Google account with your Google email address and password.
7. On the unlock selection screen, choose a screen unlock method.
8. If you are prompted with the **Secure start-up** screen, tap **Yes** to require a password when the device starts.
9. Type a device password and type it again to confirm it. Tap **OK**.
10. Select one of the options for how you want your notifications to show. Tap **Done**.
11. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
12. On the next screen, tap **Enroll** and follow the instructions on the screen if you want to set up fingerprint authentication for the UEM Client and any BlackBerry Dynamics apps that you have. Otherwise, tap **Cancel**.
13. If you are signed out of your device, unlock your device to complete the BlackBerry UEM activation.
14. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
15. If you are prompted, follow the instructions on the screen to install work apps on your device.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- In the UEM Client, tap ⋮ > **About**. In the **Activated Device** section, verify that the device information and the activation time stamp are present.
- In the BlackBerry UEM Self-Service console, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activate an Android Enterprise device without access to Google Play

These steps apply to activating Android devices that don't have access to Google Play with the Work space only (Android Enterprise) and Work and personal - full control (Android Enterprise) activation types. To activate devices with the Work and personal - user privacy (Android Enterprise) activation type, see: Activate an Android Enterprise device with the Work and personal - user privacy activation type.

To initiate activation, the device must be set to factory default settings and receive the instructions to download the BlackBerry UEM Client using a QR Code or NFC.

- You can include the download location for the UEM Client in the QR code that users receive in the activation email. Users can scan the QR Code to begin the download. For more information, see Default device activation settings.
- You can pre-program an NFC sticker that users can tap to initiate device activation.
- For Android 9 and and earlier devices, users can use NFC and tap a secondary device that has the BlackBerry UEM Enroll app installed. To download and install the UEM Enroll app on the secondary device, visit support.blackberry.com/community to read article 42607.

The same secondary device or NFC sticker can be used to activate devices for multiple users.

If you want the user to initiate device activation using a QR Code, send the activation instructions for Activate an Android Enterprise device with the Work and personal - full control activation type using a managed Google Play account to the device user.

If you want users to initiate device activation using NFC, send the following activation instructions to the device user:

Before you begin:

- Your device administrator sent you one or more email messages with the information that you need to activate your device. If you received an activation QR Code from your administrator, you can use it to activate your device and you don't need to type any information. If you did not receive a QR Code, make sure you received the following information:
  - Your Work email address
  - BlackBerry UEM activation username (usually your work user name)
  - BlackBerry UEM activation password
  - BlackBerry UEM server address (if required)
- You administrator will provide a pre-programmed NFC sticker or a secondary device that has the UEM Enroll app installed.

1. On the device that you want to activate, if you do not see the device setup Welcome screen, reset your device to the factory default settings.
2. Do one of the following:

Task	Steps
Initiate activation with an NFC sticker	**a.** Tap the device to the NFC sticker provided by your administrator. The device downloads and installs the UEM Client. **b.** Follow the prompt as the device prepares for activation.
Initiate activation with a secondary device	**a.** On the secondary device, open the UEM Enroll app. Make sure that NFC is enabled on the device. **b.** Tap **Activate device**. **c.** Tap the backs of both devices together. When you are prompted, tap anywhere on the screen of the secondary device.

Task	Steps
	d. On the device that you want to activate, follow the instructions on the screen to download and install the UEM Client.

3. Read the license agreement and tap the **I accept the License Agreement** checkbox.
4. Do one of the following:

Task	Steps
Use a QR Code to activate the device	**a.** Tap . **b.** Tap **Allow** to allow the UEM Client to take pictures and record video. **c.** Scan the QR Code in the activation email message that you received.
Manually activate the device	**a.** Type your work email address. Tap **Next**. **b.** Type your activation password. Tap **Activate My Device**. **c.** If necessary, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service. Tap **Next**. **d.** If necessary, type your username and activation password. Tap **Next**.

5. Wait while the profiles and settings are pushed to your device.
6. On the **Set up your profile** screen, tap **Set up** and wait while a work profile is set up on the device.
7. On the unlock selection screen, choose a screen unlock method.
8. If you are prompted with the **Secure start-up** screen, tap **Yes** to require a password when the device starts.
9. Type a device password, and type it again to confirm it. Tap **OK**.
10. Select one of the options for how you want your notifications to show. Tap **Done**.
11. Create a UEM Client password and tap **OK**. If you are using BlackBerry Dynamics apps, you will also use this password to sign in to all of your BlackBerry Dynamics apps.
12. On the next screen, tap **Enroll** and follow the instructions on the screen if you want to set up fingerprint authentication for the UEM Client and any BlackBerry Dynamics apps you have. Otherwise, tap **Cancel**.
13. If you are signed out of your device, unlock your device to complete the BlackBerry UEM activation.
14. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
15. If you are prompted, follow the instructions on the screen to install work apps on your device.
16. If necessary, open the email app that your organization wants you to use and follow the instructions to set up email on your phone.

Activate an Android device with the MDM controls activation type

Note: These steps apply only to devices that are assigned the MDM controls activation type. This activation type is deprecated in Android 10. Attempts to activate Android 10 and later devices with the MDM controls activation type will fail. For more information, visit https://support.blackberry.com/community to read article 48386.

Send the following activation instructions to the device user.

1. On the device, install the BlackBerry UEM Client from Google Play.
2. Open the UEM Client.
3. Read the license agreement and tap the **I accept the License Agreement** checkbox.
4. Do one of the following:

Task	Steps
Use a QR Code to activate the device	**a.** Tap . **b.** Tap **Allow** to allow the UEM Client to take pictures and record video. **c.** Scan the QR Code in the activation email message that you received.
Manually activate the device	**a.** Type your work email address. Tap **Next**. **b.** Type your activation password. Tap **Activate My Device**. **c.** If necessary, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service. Tap **Next**. **d.** If necessary, type your username and activation password. Tap **Next**.

5. Tap **Next**.
6. Tap **Activate** to activate the device administrator. You must activate the device administrator to access work data on your device.
7. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
8. If you are prompted, follow the instructions on the screen to install work apps on your device.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- In the UEM Client, tap > **About**. In the **Activated Device** section, verify that the device information and the activation time stamp are present.
- In the BlackBerry UEM Self-Service console, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activating iOS devices

The information that users must enter and the steps to activate iOS and iPadOS devices may be different depending on the iOS version and whether the activation type includes MDM controls. The activation email templates contain the information that users need. You can update the text in the email templates if necessary. For more information, see Email templates.

Activate an iOS or iPadOS device with the MDM controls activation type

These steps apply to iOS and iPadOS devices that are activated using MDM controls or User privacy with MDM options enabled.

During activation, users must leave the BlackBerry UEM Client app to manually install the MDM profile. Lockdown Mode must be disabled on the device (iOS andiPadOS 16 or later). Lockdown Mode prevents the installation of configuration profiles which are required for activation.

Send the following activation instructions to the device user, or send them a link to the following workflow: Activating your iOS device.

Before you begin:

- If Lockdown Mode is enabled on your device (iOS and iPadOS 16 or later), you must disable it to activate the device. Lockdown Mode prevents the installation of configuration profiles which are required for activation. If necessary, you can enable Lockdown Mode after activation.

1. On the device, install the BlackBerry UEM Client. You can download the BlackBerry UEM Client from the App Store.
2. On the device, tap **UEM Client** and accept the License Agreement.
3. Do one of the following:

Task	Steps
Use a QR Code to activate the device	**a.** Tap  . **b.** Tap **Allow** to allow the BlackBerry UEM Client to take pictures and record video. **c.** Scan the QR Code in the activation email message that you received.
Manually activate the device	**a.** Type your work email address and activation password. **b.** If necessary, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service. **c.** Tap **Next**.

4. Tap **Allow** to allow the UEM Client to send you notifications. Choosing **Don't Allow** will prevent the device from activating completely.
5. When you are prompted to install a configuration profile, tap **OK**.
6. When you are prompted to download the configuration profile, tap **Allow**.
7. After the download is complete, open **Settings**.
8. Tap **General** and navigate to **Profiles and Device Management**.
9. To install the profile, tap **BlackBerry UEM Profile** and follow the instructions on the screen.
10. After the installation is complete, return to the BlackBerry UEM Client app to complete the activation.
11. If you are prompted, follow the instructions on the screen to install work apps on your device.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- On the device, open the BlackBerry UEM Client app and tap **About**. In the Activated Device and Compliance Status sections, verify that the device information and the activation time stamp are present.
- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activate an iOS or iPadOS device with Apple User Enrollment

Apple User Enrollment is supported on devices running iPad and iPadOS 13.1 or later.

To start enrollment, users use the camera app on the device to scan a QR Code provided in the Apple User Enrollment activation email to manually download and install the MDM profile to the device. To activate their device, users log in to their managed Apple ID account that matches the email address of the BlackBerry UEM user account. You should assign the UEM Client using a VPP license to users if you want to allow them to easily activate other BlackBerry Dynamics apps, import certificates, use BlackBerry 2FA features, use CylancePROTECT, and check their compliance status. The UEM Client setup starts when the user accepts the license agreement.

Send the following activation instructions to the device user.

Before you begin:

- Verify that you received an activation email that has the QR Code for Apple User Enrollment. If you didn't receive the email, contact an administrator.
- If your device is already activated with BlackBerry UEM, you must deactivate your device.

- Uninstall the BlackBerry UEM Client.
- You must have a managed Apple ID account that is managed through your organization.
- Your device must not be a supervised device. If your device is supervised, it is noted in the Settings app near your Apple ID.
- If Lockdown Mode is enabled on your device (iOS and iPadOS 16 or later), you must disable it to activate the device. Lockdown Mode prevents the installation of configuration profiles which are required for activation. If necessary, you can enable Lockdown Mode after activation.

1. Open the activation email that contains the QR Code for Apple User Enrollment. If the QR Code already expired, you can request a new activation code from BlackBerry UEM Self-Service or contact your administrator.
2. Open the Camera app on your device and scan the QR code in the activation email. When you are prompted, tap the notification to open the URL in Safari.
3. When you are prompted to download the UEM configuration profile, tap **Allow**.
4. After the download is complete, tap **Close**.
5. Go to **Settings** > **General** > **Profile**.
6. Tap **UEM profile**.
7. On the User Enrollment screen, tap **Enroll my iPhone** or **Enroll my iPad**.
8. Type your passcode.
9. Log in to Apple ID using your managed Apple ID credentials.
10. If your administrator assigned the BlackBerry UEM Client app to you, tap **Install** when prompted or open Work Apps.
11. To set up the BlackBerry UEM Client app, open it and accept the license agreement. Follow the instructions on the screen to complete the activation process.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- On the device, open the BlackBerry UEM Client app and tap **About**. In the Activated Device and Compliance Status sections, verify that the device information and the activation time stamp are present.
- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activate a macOS device

Send the following activation instructions to the device user.

Before you begin: You need the following BlackBerry UEM Self-Service login information:

- Web address for BlackBerry UEM Self-Service
- Username and password
- Domain name

1. Using the device that you want to activate, and the login information that you received from your administrator, log in to BlackBerry UEM Self-Service.
2. If there are already devices displayed, click **Activate a device**.
3. In the Device drop-down menu, click **macOS**.
4. Watch the activation tutorial.
5. Click **Submit**.
6. Follow the instructions to install the required profiles and to complete the activation of the device. When the activation completes, you can see your device displayed in BlackBerry UEM Self-Service.

Activate an Apple TV device

Send the following activation instructions to the device user.

Before you begin:

- You need the web address and your login credentials for BlackBerry UEM Self-Service.
- You need a macOS computer with Apple Configurator 2 installed.
- You need a USB-C or Micro-USB cable (depending on the version of Apple TV).
- Verify that the Apple TV device is in supervised mode.
- Disconnect the HDMI cable and power cord from the Apple TV device.

1. Connect the Apple TV device to your macOS computer using a USB-C or Micro-USB cable.
2. For third and fourth generation versions of Apple TV, connect the power cord.
3. On your macOS computer, log in to BlackBerry UEM Self-Service.
4. Depending on whether you are activating your first device, or you already have an activated device, click  or click  > **Activate a device**.
5. In the Device drop-down menu, click **Apple TV**.
6. Click **Submit**.
7. Click **Download profile**.
8. Click **Close**.
9. Open Apple Configurator 2.
10. Select Apple TV and click **Add > Profiles**.
11. Select the configuration file that you downloaded in Step 7 and click **Add**.
12. When the activation completes, you can see your device displayed in BlackBerry UEM Self-Service.

Activate a Windows 10 tablet or computer

Note: If you want to manage Windows 10 devices using MDM, the devices cannot be managed by Microsoft System Center Configuration Manager.

Send the following activation instructions to the device user.

1. In the browser on your device, type or paste the certificate server address. You can find the certificate server address in the activation email you received. If you did not receive a link to the certificate, contact your administrator for assistance.
2. Click **Save**.
3. In the certificate download notification, tap **Open**.
4. Click **Open**.
5. Click **Install Certificate**.
6. Select the **Current User** option. Click **Next**.
7. Select the **Place all certificates in the following store** option. Click **Browse**.
8. Select **Trusted Root Certification Authorities**. Click **OK**.
9. Click **Next**.
10. Click **Finish**.
11. Click **OK**.

12. Click **OK**.
13. Click the **Start** button.
14. Perform one of the following tasks:

Device OS version	Steps
Windows 10 version 1607 or later	**a.** Tap **Settings > Accounts > Access work or school**. **b.** Tap **Enroll only in device management**.
Windows 10 version earlier than 1607	**a.** Tap **Settings > Accounts > Work access**. **b.** Tap **Connect**.

15. In the **Email address** field, type your email address. Tap **Continue**.
16. If you are prompted, in the **Server** field, type the server name and tap **Continue**. You can find the server name in the activation email that you received from your administrator or in BlackBerry UEM Self-Service when you set your activation password.
17. In the **Activation password** field, type your activation password and tap **Continue**. You can find your activation password in the activation email that you received from your administrator, or you can set your own activation password in BlackBerry UEM Self-Service.
18. Tap **Done**.
19. The activation process is complete.

After you finish:

- To verify that the activation process completed successfully, you can perform the following actions:
  - On the device, click Settings > Accounts > Access work or school (or Work access) to confirm that your device is connected to BlackBerry UEM. Click the briefcase icon > Info to check the sync status information.
  - In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.
- If requested by your administrator, add your work account to Accounts used by other apps so that you can access required online apps.
  - For Windows 10 version 1607 or later, click Settings > Accounts > Access work and school > Connect. Type your work email address and password.
  - For Windows 10 version earlier than 1607, click Settings > Accounts > Your email and accounts. Under Accounts used by other apps, click Add a work or school account, and type your work email address and password.

Configure support for Android zero-touch enrollment

Zero-touch enrollment allows you to deploy a large number of Android Enterprise devices at one time.

Your organization purchases these devices from an authorized enterprise reseller, who sets up a zero-touch enrollment account and adds the devices to the account to provision them for device management. When users set up one of these devices for the first time or reset a device to factory settings, the device automatically downloads the BlackBerry UEM Client and starts the activation process with BlackBerry UEM. If the user restarts the device before activation is complete, cancels the activation, or allows the battery to drain before activation is complete, the device automatically resets to factory settings and the activation process restarts. Users can't display the device home screen to use device features until activation is complete.

To use zero-touch enrollment in BlackBerry UEM, devices must have been enabled for zero-touch enrollment. For more information about zero-touch enrollment and how to configure it, see the Android Enterprise Help and https://support.google.com/work/android/answer/7514005.

1. Purchase supported devices from an approved enterprise reseller. The reseller sets up a zero-touch enrollment account for your organization.
2. In the zero-touch platform, the reseller adds the devices that you purchased.
3. In the management console, on the menu bar, click **Settings > External integration**.
4. Click **Android Enterprise**.
5. Click **Launch zero-touch console**.
6. If this is the first time you have connected to Android Zero Touch with UEM, click **Next** and sign in to Google using the address associated with your organization's zero-touch account.
   The Android settings for managing zero-touch enrollment display in UEM.
7. Create or manage configurations and assign them to the devices that you purchased.

   You can also open the Android zero-touch portal to manage enrollment configurations there.

After you finish:

- In BlackBerry UEM, verify that the appropriate profiles and IT policies are assigned to users. To use zero-touch enrollment, you must assign an activation profile with the "Work and personal - full control (Android Enterprise)" or "Work space only (Android Enterprise) " activation type enabled.
- Distribute the devices to users.

Activate multiple devices using Knox Mobile Enrollment

Samsung Knox Mobile Enrollment allows you to deploy large numbers of Samsung Knox devices at one time. For more details, refer to the information from Samsung: https://www.samsungknox.com/en/products/knox-mobile-enrollment.

Knox Mobile Enrollment does not support device admin based enrollment on devices running Android 11 or later. For more details, refer to the information from Samsung: https://docs.samsungknox.com/admin/knox-mobile-enrollment/release-notes/November-4-2020.htm

Your organization purchases these devices from an authorized reseller or a reseller that is willing to share the device IMEIs directly with Samsung so that the device can use Knox Mobile Enrollment. When users set up one of these devices for the first time or reset a device to factory settings, the device automatically downloads the BlackBerry UEM Client and starts the activation process with BlackBerry UEM. If the user restarts the device before activation is complete, cancels the activation, or allows the battery to drain before activation is complete, the device automatically resets to factory settings and the activation process restarts. Users can't display the device home screen to use device features until activation is complete.

1. On the menu bar, click **Settings > External integration**.
2. Click **KNOX Mobile Enrollment**.
3. Complete the steps on the screen.

After you finish: After you have completed the activation, click **Download** to download the configuration.json file. In the file, compare the entry in the CFPrint section with the entry that you added when you configured Knox Mobile Enrollment. If the entries are different, copy the entire text from the .json file into the Custom JSON Data field on the Knox Mobile Enrollment page.

Restricting unsupervised iOS devices

There are two ways to restrict unsupervised iOS devices in BlackBerry UEM:

- Use Apple DEP devices that have supervised mode enabled by default. Supervised mode cannot be disabled on Apple DEP devices.
- You can assign an activation profile that has the "Do not allow unsupervised devices to activate" setting selected to user accounts. This setting is supported for the "MDM controls" and "User privacy" (with SIM-based licensing enabled) activation types. BlackBerry UEM prevents unsupervised devices from activating and automatically removes devices if they become unsupervised, whether the devices are activated with the BlackBerry UEM Client or using DEP. For more information, see Create an activation profile.

Import or export a list of approved device IDs

You can import and export a list of unique device identifiers to restrict which devices can enroll with BlackBerry UEM. Currently, the only unique identifier that BlackBerry UEM supports is the device serial number.

CAUTION: LG devices do not support this feature.

Before you begin: To import a list, ensure you have a .csv file that contains the list of unique device identifiers.

1. Navigate to **Settings > General settings > Activation defaults**.
2. In the **Import or export device IDs** section, beside the **Upload approved device IDs (.csv)** field, click **Browse**.
3. Navigate to your organization's .csv file.
4. Click **Open**.
5. Click **Save**.
6. After you have imported the list, to export the list, click **Export approved device IDs (.csv)**.

Activating iOS devices that are enrolled in DEP

You can enroll iOS and iPadOS devices in Apple's Device Enrollment Program and assign enrollment configurations to devices using the BlackBerry UEM management console. The enrollment configurations include extra rules that are assigned to the devices during MDM enrollment.

You can use an Apple Business Manager account to synchronize BlackBerry UEM with DEP. Apple Business Manager is a web-based portal in which you can enroll and manage iOS devices in DEP, and manage Apple VPP accounts. If your organization uses DEP or VPP, you can upgrade to Apple Business Manager.

When the devices are activated, BlackBerry UEM sends IT policies and profiles that you assigned to users.

Steps to activate devices that are enrolled in DEP

When you activate iOS devices that are enrolled in Apple's Device Enrollment Program, you perform the following actions:

Step	Action
1	Register iOS devices in DEP and assign them to the BlackBerry UEM server.
2	If you did not select "Automatically assign new devices to this configuration" when you created the enrollment configuration, or you want to assign a different configuration, assign an enrollment configuration.
3	Optionally, add the BlackBerry UEM Client to the app list and assign it to user accounts or user groups. See Add an iOS app to the app list.
4	If you do not want to use the default activation profile, see Create an activation profile and assign it to a user account or to a group that the user belongs to. Optionally, Assign an activation profile to iOS devices.
5	Set an activation password for the user and send an activation email to users using the Apple DEP email template. When you set the activation password, you must select the "Default device activation" option. Company directory users can use their company directory usernames and passwords so you don't need to create an activation password. Users must enter their usernames in the format domain\username (the credentials match your organization's domain and username variables (“%UserDomain%/%UserName%”)). For more information about variables see the Default variables topic. Users can also enroll using their email address and Active Directory password. Optionally, you can Assign a user to an iOS device. When you assign a user to the device in BlackBerry UEM, they are not prompted for a username or password during device activation.

Step	Action
6	Distribute the devices to users and have them complete the setup. After the setup completes, users must install and open the BlackBerry UEM Client.

Register iOS devices in DEP and assign them to the BlackBerry UEM server

To register the devices, you must enter the device serial numbers in the Apple Business Manager or DEP Portal and assign the devices to the BlackBerry UEM server. You can enter the serial numbers in the following ways:

- Type in each number
- Select the order number that Apple assigned to the devices when you purchased them
- Upload a .csv file containing the serial numbers

Before you begin: Configure BlackBerry UEM to use DEP. For more information, see the on-premises Configuration content or the UEM Cloud Configuration content.

1. In a browser, type **business.apple.com** or **deploy.apple.com**.
2. Sign in to your Apple Business Manager or DEP account.
3. In the **Device Enrollment Program** section, click **Manage Devices**.
4. Follow the steps to enter the serial numbers for the devices.
5. Assign the serial numbers to the BlackBerry UEM server.

After you finish: Assign an enrollment configuration to iOS devices.

Assign an enrollment configuration to iOS devices

If you created an enrollment configuration and selected "Automatically assign all new devices to this configuration," BlackBerry UEM automatically assigns the configuration when DEP devices synchronize with UEM. Otherwise, you must assign an enrollment configuration to devices. UEM synchronizes with DEP on a daily schedule and whenever you view the Apple DEP devices page.

If the activation status for a device is still pending, you can remove an existing enrollment configuration and assign a new one.

In the BlackBerry UEM management console, the following icons indicate the status of enrollment configurations:

Status	Icon
✓	An enrollment configuration is assigned. BlackBerry UEM also displays a check mark for activated devices if the applied DEP enrollment configuration was updated or resaved in the Apple Device Enrollment Program External Integration settings after the device was activated. If the configuration is updated, UEM can't confirm that enrollment configuration used when the device was activated matches the assigned configuration.
?	No enrollment configuration is assigned.

Status	Icon
	An enrollment configuration is applied, but it is pending activation.
	Activation was successful.

Before you begin: Register iOS devices in DEP and assign them to the BlackBerry UEM server.

1. On the menu bar, click **Users > Apple DEP devices**.
2. Select the check boxes beside the devices that you want to assign an enrollment configuration to. You must select devices that are registered to the same DEP account.
3. Click .
4. In the **Enrollment configuration** drop-down list, select the enrollment configuration that you want to assign.
5. Click **Assign**.

After you finish:

Distribute the iOS devices to users. As part of the device setup, devices are activated with UEM. Users are prompted for a username and password. Company directory users can use their company directory username (in the format domain\username) and password. Local users need to use an activation password. See Set an activation password and send an activation email message.

Add an enrollment configuration

An enrollment configuration allows you to define how devices that are enrolled in DEP are set up when they are activated in BlackBerry UEM. You can create as many enrollment configurations as your organization needs.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. Click the name of a DEP account.
4. In the **DEP enrollment configurations** section, click +.
5. Type a name for the configuration.
6. Complete one of the following tasks:
   - If you want BlackBerry UEM to automatically assign the enrollment configuration when DEP devices synchronize to BlackBerry UEM, select the "Automatically assign all new devices to this configuration" checkbox. BlackBerry UEM synchronizes with Apple DEP on a daily schedule and whenever you view the Apple DEP devices page.

     Note: If you previously created an enrollment configuration with this setting and the configuration was applied to devices, BlackBerry UEM does not assign the new enrollment configuration.

     Note: You can select only one enrollment configuration to be automatically assigned to new DEP devices. If you previously created an enrollment configuration with this setting, the setting is removed from the previous configuration and added to the new one.
   - If you want to manually assign the enrollment configuration to specific devices, leave the "Automatically assign all new devices to this configuration" box unchecked.
7. Optionally, type a department name and support phone number to be displayed on devices during setup.
8. In the **Device configuration** section, select from the following options:
   - Allow pairing - if selected, users can pair the device with a computer

- Mandatory - if selected, users are not prompted to accept the enrollment configuration
- Allow removal of MDM profile - if selected, users can deactivate devices.
- Wait until device is configured - if selected, users cannot cancel the device setup until activation with BlackBerry UEM is completed.

9. In the **Skip during setup** section, select the items that you do not want to include in the device setup:
   - Passcode - if selected, users aren't prompted to create a device passcode
   - Location services - if selected, location services are disabled on the device
   - Restore - if selected, users can't restore data from a backup file
   - Move from Android - if selected, users can't restore data from an Android device
   - Apple ID - if selected users are prevented from signing in to Apple ID and iCloud
   - Terms and conditions - if selected, users don't see the iOS terms and conditions
   - Siri - if selected, Siri is disabled on devices
   - Diagnostics - if selected, diagnostic information isn't automatically sent from the device during setup
   - Biometric - if selected, users can't set up Touch ID
   - Payment - if selected, users can't set up Apple pay
   - Zoom - if selected, users can't set up Zoom
   - Home button setup - if selected, users can't adjust the Home button's click
   - Device-to-device migration - if selected, users can't transfer data from their previous device to their new device
10. Click **Save**.
11. If you selected "Automatically assign new devices to this configuration," click **Yes**.

After you finish: If you did not select "Automatically assign new devices to this configuration", see Assign an enrollment configuration to iOS devices.

Remove an enrollment configuration that is assigned to iOS devices

If you assigned an enrollment configuration to devices and the configuration is not yet applied to the devices, you can remove the enrollment configuration from the devices.

1. On the menu bar, click **Users > Apple DEP devices**.
2. Select the check boxes beside the devices that you want to remove an enrollment configuration from. You must select devices that are registered to the same DEP account.
3. Click .
4. Click **Remove**.

After you finish: Assign an enrollment configuration to iOS devices.

Delete an enrollment configuration

If you delete an enrollment configuration that is assigned to devices before the configuration is applied to the devices, BlackBerry UEM removes the enrollment configuration assigned to the device records.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. Click the name of a DEP account.
4. In the **DEP enrollment configurations** section, click ✕.

5. Click **Delete**.

After you finish: If BlackBerry UEM removes the enrollment configuration from devices, assign an enrollment configuration to the devices.

Change the settings for an enrollment configuration

If you assigned an enrollment configuration to devices and the configuration is not applied to the devices, BlackBerry UEM updates the enrollment configuration assigned to the devices when you save the changes to the configuration.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. Click the name of a DEP account.
4. In the **DEP enrollment configurations** section, click the name of the configuration you want to change.
5. Change the settings.
6. Click **Save**.

View the settings for an enrollment configuration that is assigned to a device

If an enrollment configuration is assigned to an iOS device and the configuration is pending, you can view the settings for the enrollment configuration.

1. On the menu bar, click **Users > Apple DEP devices**.
2. In the **Enrollment configuration** column, click the name of an enrollment configuration.

Assign an activation profile to iOS devices

You can assign a specific activation profile to each device registered in Apple DEP. For example, if a user has multiple iOS devices that require different activation types, you can specify the activation profile for each device. When a device is activated, the activation profile that is assigned to it takes precedence over the activation profile that is assigned to the user account.

Before you begin: Create an activation profile.

1. On the menu bar, click **Users** > **Apple DEP devices**.
2. Select the check boxes beside the devices that you want to assign an activation profile to. You must select devices that are registered to the same DEP account.
3. Click .
4. In the **Activation profile** drop-down list, select an activation profile.
5. Click **Assign**.

Remove an activation profile that is assigned to iOS devices

When you remove an activation profile that is assigned to an Apple DEP device, the activation profile that is assigned to the user account takes effect.

1. On the menu bar, click **Users** > **Apple DEP devices**.
2. Select the check boxes beside the devices that you want to remove the activation profile from. You must select devices that are registered to the same DEP account.
3. Click .
4. Click **Remove**.

Assign a user to an iOS device

You can assign a user directly to a device registered in Apple DEP before the device is activated. When you assign a user directly to the device, they are not prompted for a username or password during device activation.

1. On the menu bar, click **Users > Apple DEP devices**.
2. In the **User Association** column for the device that you want to assign, click **Select**.
3. In the **Select user** search box, search for the user that you want to assign to the device.
4. In the list of search results, click the user account.
5. Click **Save**.

Unassign a user from an iOS device

1. On the menu bar, click **Users > Apple DEP devices**.
2. In the **User association** column, click the username link for the device that you want to remove the user from.
3. Click **Unassign**.

View the owner of an activated device

After a device is successfully activated, you can view the owner of the device.

1. On the menu bar, click **Users > Apple DEP devices**.
2. In the **User association** column, click the username link.

Activating iOS devices using Apple Configurator 2

If you have BlackBerry UEM in an on-premises environment, you can use Apple Configurator 2 to prepare iOS and iPadOS devices for activation in BlackBerry UEM. Users can activate the prepared devices without using the BlackBerry UEM Client app. They need only their username and activation password.

When the devices are activated, BlackBerry UEM sends the IT policy and profiles that you assigned to users to the devices.

Apple Configurator is not supported by BlackBerry UEM Cloud.

Note: For certain features to work, you must assign the BlackBerry UEM Client app to the users. Users must start the BlackBerry UEM Client after they activate the device. For information about when you need to assign the BlackBerry UEM Client app to users, visit support.blackberry.com/community to read article 39313.

Steps to activate devices using Apple Configurator 2

Step	Action
1	Optionally, add the BlackBerry UEM Client app to the app list and assign it to user accounts or user groups. See Add an iOS app to the app list.
2	Add BlackBerry UEM server information to Apple Configurator 2.
3	Prepare iOS devices using Apple Configurator 2.
4	Create an activation profile and assign it to a user account or group.
5	Set an activation password and send an activation email message.
6	Distribute the devices to users and have them complete the setup. To enforce a compliance profile, users must install and open the BlackBerry UEM Client app after the setup is complete.

Add BlackBerry UEM server information to Apple Configurator 2

Before you begin: Download and install the latest version of Apple Configurator 2 from Apple.

1. In the Apple Configurator 2 menu, select **Preferences > Servers**.
2. Click + > **Next**.
3. In the **Name** field, type a name for the server.

4. In the **Hostname or URL** field type the BlackBerry UEM server URL using the format: *<http or https>://<servername>:<port>*, where the default port number is 8885. For more information about port settings, see BlackBerry UEM listening ports in the Planning content.
5. Click **Next**.
6. Close the **Server** window.

Prepare iOS devices using Apple Configurator 2

When you prepare a device, Apple Configurator 2 wipes the device and upgrades the device OS to the latest version.

Before you begin: Add BlackBerry UEM server information to Apple Configurator 2.

1. Open Apple Configurator 2.
2. Connect one or more iOS devices to your computer.
3. Click **Prepare**.
4. In the **Configuration** drop-down list, select **Manual**. Click **Next**.
5. In the **Server** drop-down list, select the BlackBerry UEM server. Click **Next**.
6. Optionally, select the **Supervise devices** checkbox. Click **Next**.
7. If you selected **Supervise devices**, complete the organization information.
8. Click **Prepare** and wait while the device is prepared. The process can take up to 15 minutes.

After you finish: Distribute the devices to users for activation.

Tips for troubleshooting device activation

When you troubleshoot activation of any device type, always check the following:

- Make sure that BlackBerry UEM supports the device type. For more information about supported device types, see the Compatibility matrix.
- Make sure that there are licenses available for the device type the user activates and the activation type that is assigned to the user. For more information, see the Licensing content.
- Check network connectivity on the device.
  - Verify that the mobile or Wi-Fi network is active and has sufficient coverage.
  - If the user must manually configure a VPN or work Wi-Fi profile to access content behind your organization's firewall, make sure that the user's profiles are configured correctly on the device.
  - If on work Wi-Fi, make sure that the device network path is available. For more information on configuring network firewalls to work with BlackBerry UEM, visit support.blackberry.com/community to read article 36470.
- Make sure that the activation profile assigned to the device supports the device type being activated.
- If you have defined compliance rules for devices with a jailbroken or rooted OS, restricted OS versions, or restricted device models, verify that the device is compliant.
- If BlackBerry UEM is installed on-premises and the device is trying to connect with BlackBerry UEM or the BlackBerry Infrastructure through your organization's firewall, verify that the proper firewall ports are open. For more information about required ports, see the Planning content.
- Gather device logs:
  - For more information on retrieving iOS device log files, visit support.blackberry.com/community to read article 36986.
  - For more information on retrieving Android device log files, visit support.blackberry.com/community to read article 32516.

Knox Workspace and Android Enterprise devices

When you troubleshoot activation of Samsung devices that use Samsung Knox Workspace, check the following:

- Make sure the device supports Knox Workspace. See the information from Samsung.
- Make sure that the Warranty Bit has not been triggered. See the information from Samsung.
- Make sure that the Knox container version is supported. Knox Workspace requires Knox Container 2.0 or later. For more information about supported Samsung Knox versions, see the list from Samsung.

When you troubleshoot activation of Android Enterprise devices, check the following:

- Make sure the device supports Android Enterprise. For more information, visit https://support.google.com/work/android/answer/6174145 to read article 6174145.
- Make sure that there is an available license and the activation type is set to Work and personal - user privacy .
- To use the Work and personal - user privacy activation type, devices must be running Android OS version 5.1 or later.

- Make sure that the user account in BlackBerry UEM has the same email address as the one in the Google domain. If the email addresses do not match, the device will show the following error: Unable to activate device - Unsupported activation type. Look for the following in the core log file:
  - ```
    ERROR AfW: Could not find user in Google domain. Aborting user creation and
     activation.
    ```
  - ```
    ERROR job marked for quarantine due to: Unable to activate device -
     Unsupported activation type
    ```

Device activation can't be completed because the server is out of licenses. For assistance, contact your administrator.

Description

This error is displayed on the device during activation when licenses are not available or the licenses have expired.

Possible solution

In BlackBerry UEM, perform the following actions:

- Verify that licenses are available to support activation.
- If necessary, activate licenses or purchase additional licenses.

For more information, see "Managing licenses for devices".

Please check your username and password and try again

Description

This error is displayed on a device during activation when a user has entered an incorrect username, password, or both.

Possible solution

Enter the correct username and password.

Profile failed to install. The certificate "AutoMDMCert.pfx" could not be imported.

Description

This error is displayed on an iOS device during activation when a profile already exists on the device.

Possible solution

Go to **Settings > General > Profiles** on the device and verify that a profile already exists. Remove the profile and reactivate. If the issue persists, you might have to reset the device because data might be cached.

Profile Installation Failed: The new MDM payload does not match the old payload.

Description

This error is displayed on an iOS device during activation when a profile already exists on the device.

Possible solution

Go to **Settings > General > Profiles** on the device and verify that a profile already exists. Remove the profile and reactivate. If the issue persists, you might have to reset the device because data might be cached.

Error 3007: Server is not available

Description

This error can appear on the device during activation because of the following:

- The certificate that BlackBerry UEM uses to sign the MDM profile that it sends to iOS devices is not trusted by the device. The user is asked to trust this certificate when they activate the device.
- If you configure a transparent proxy such as Blue Coat and it monitors port 443 for non-standard traffic, the BlackBerry UEM Client cannot make the required HTTP CONNECT and HTTP OPTIONS calls to BlackBerry UEM.

Possible solutions

Possible solutions include:

- In an on-premises environment, install the root certificate for the CA that issued the certificate that BlackBerry UEM uses to sign the MDM profile to the iOS device. For more information about this certificate, see the on-premises Configuration content.
- Verify that your proxy configuration is not blocking the BlackBerry UEM Client from making HTTP CONNECT and HTTP OPTIONS calls to BlackBerry UEM. For more information, visit support.blackberry.com/community to read article 38644.

Unable to contact server, please check connectivity or server address

Description

This error can appear on the device during activation because of the following:

- The username was entered incorrectly on the device.

- The customer address for device activation was entered incorrectly on the device.

  Note: This is only required when registration with the BlackBerry Infrastructure has been disabled.
- No activation password has been set, or the password has expired.

Possible solutions

Possible solutions include:

- Verify the username and password.
- Verify the customer address for device activation.
- Set a new activation password using BlackBerry UEM Self-Service.

iOS or macOS device activations fail with an invalid APNs certificate

Possible cause

If you are unable to activate iOS or macOS devices, the APNs certificate may not be registered correctly.

Possible solution

Perform one or more of the following actions:

- In the management console, on the menu bar, click **Settings > External integration > Apple Push Notification**. Verify that the APNs certificate status is "Installed." If the status is not correct, try to register the APNs certificate again.
- To test the connection between BlackBerry UEM and the APNs server, click **Test APNS certificate**.
- If necessary, obtain a new signed CSR from BlackBerry, and request and register a new APNs certificate.

Users are not receiving the activation email

Description

Users are not receiving their activation email, even though all of the settings in BlackBerry UEM are correct.

Possible solution

If users are using a third-party mail server, email messages from BlackBerry UEM can be marked as spam and end up in the spam email folder or the junk mail folder.

Make sure that users have checked their spam email folder or junk mail folder for the activation email.

User details screen is showing more Windows devices activated with UEM than expected

Description

When a user installs BlackBerry Access and BlackBerry Work for Windows on a computer, BlackBerry Access and BlackBerry Work for Windows appear as a "Windows device" on the User details screen in the BlackBerry UEM management console. This is expected behavior.

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