



BlackBerry UEM

Managing Android devices

Administration

12.17

Contents

| | |
|--|-----------|
| Managing Android devices..... | 5 |
| Managing wearable devices..... | 5 |
| What you can control on Android devices..... | 6 |
| Steps to manage Android devices..... | 8 |
| Supporting Android Enterprise activations..... | 9 |
| Support Android Enterprise activations using managed Google Play accounts..... | 9 |
| Support Android Enterprise activations with a G Suite domain..... | 10 |
| Support Android Enterprise activations with a Google Cloud domain..... | 10 |
| Support Android Enterprise devices without access to Google Play..... | 11 |
| Program an NFC sticker to activate devices..... | 13 |
| Specify the default activation settings..... | 13 |
| Default device activation settings..... | 14 |
| Controlling Android devices with an IT policy..... | 16 |
| Setting Android password requirements..... | 16 |
| Android: Global password rules..... | 17 |
| Android: Work profile password rules..... | 19 |
| Controlling Android devices with profiles..... | 22 |
| Profiles reference - Android devices..... | 23 |
| Managing apps on Android devices..... | 26 |
| App behavior on Android Enterprise devices..... | 26 |
| Activating Android devices..... | 28 |
| Activation types: Android devices..... | 30 |
| Creating activation profiles..... | 34 |
| Create an activation profile..... | 35 |
| Import or export a list of approved device IDs..... | 36 |
| Supporting Samsung Knox DualDAR..... | 36 |
| Activate an Android Enterprise device with the Work and personal - user privacy activation type..... | 37 |
| Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain..... | 39 |
| Activate an Android Enterprise device with the Work space only activation type using a managed Google Play account..... | 40 |
| Activate an Android Enterprise device with the Work and personal - full control activation type using a managed Google Play account..... | 41 |

| | |
|--|-----------|
| Activate an Android Enterprise device without access to Google Play..... | 42 |
| Activate an Android device with the MDM controls activation type..... | 44 |
| Managing and monitoring activated Android devices..... | 46 |
| Commands for Android devices..... | 46 |
| Enable users to unlock a BlackBerry Dynamics app using a third-party identity provider..... | 50 |
| Legal notice..... | 51 |

Managing Android devices

BlackBerry UEM provides precise management of how Android devices connect to your network, what device capabilities are enabled, and what apps are available. Whether devices are owned by your organization or your users, you can provide mobile access to your organization's information while protecting it from anyone who should not have access.

This guide describes the options you have to manage Android devices and helps you find the details you need to take advantage of all available features.

Managing wearable devices

You can activate and manage certain Android based wearable devices in BlackBerry UEM. Wearable devices, such as smart glasses provide users with hands-free access to visual information such as notifications, step-by-step instructions, images, and video and allow users to issue voice commands, scan barcodes and use GPS navigation.

BlackBerry UEM supports the following wearable devices:

- Vuzix M300 Smart Glasses

To manage wearable devices, follow the instructions for Android devices. The following BlackBerry UEM features are supported for wearable devices:

- Device activation using a QR Code
- IT policies
- Wi-Fi, VPN, enterprise connectivity, compliance, and certificate profiles
- BlackBerry Secure Connect Service
- Device commands
- App management
- Device groups
- Location services

Wearable devices use the BlackBerry UEM Client for activation. You can activate wearable devices using a QR code instead of an activation password.

What you can control on Android devices

BlackBerry UEM provides all of the tools you need to control the features that Android devices allow you to manage. It also includes features that allow you to give device users secure access to work resources without fully managing the device.

| Control level | Description |
|--|---|
| Unmanaged devices User privacy activations | <p>You can activate a device on BlackBerry UEM with the "User privacy" activation type to provide secure access to work resources without managing the device. This option is often used for BYOD devices.</p> <p>These activations can allow users to access your network over VPN using BlackBerry 2FA, share files securely using BlackBerry Workspaces, and install BlackBerry Dynamics apps such as BlackBerry Work and BlackBerry Access to access work email and your work intranet.</p> |
| Managed devices with a work profile Work and personal - user privacy (Android Enterprise) activations | <p>Android Enterprise devices can be managed but allow for personal use by creating a work profile on the device that separates work and personal data. This option maintains privacy for user's personal data in the personal profile but lets you manage work data using commands and IT policy rules. You can manage work apps on the device, including BlackBerry Dynamics apps.</p> <p>You can wipe work data, but not personal data, from the device. Work and personal data are both protected using encryption and password authentication. This option is often used for corporate-owned, personally enabled (COPE) and BYOD devices.</p> |
| Fully managed devices with a work profile Work and personal - full control (Android Enterprise) activations | <p>Android Enterprise devices can be fully managed but allow for some personal use by creating a work profile on the device that separates work and personal data but allows your organization to maintain full control over the device and wipe all data from the device. Some IT policy rules can be applied separately to the work and personal profiles. You can manage work apps on the device, including BlackBerry Dynamics apps.</p> <p>You can log SMS, MMS, and phone calls sent and received on the device (if it runs Android 10 or earlier). Work and personal data are both protected using encryption and password authentication. This option is often used for COPE devices.</p> |
| Fully managed devices Work space only (Android Enterprise) activations | <p>Android Enterprise devices can be fully managed and have a work profile but no personal profile. This option lets you manage the entire device using commands and IT policy rules. You can manage work apps on the device, including BlackBerry Dynamics apps.</p> <p>You can log SMS, MMS, and phone calls sent and received on the device. All data on the device is protected using encryption and a method of authentication such as a password. This option is often used for corporate-owned, business only (COBO) devices.</p> |

| Control level | Description |
|--|--|
| Device administration MDM controls activations | <p>You can manage Android 9.x and earlier devices 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. To provide security for work data you can install BlackBerry Dynamics apps.</p> <p>This activation type is deprecated for Android 10 devices. For more information, visit https://support.blackberry.com/community to read article 48386.</p> <p>You can use device groups and compliance profiles to manage what happens for devices activated with "MDM controls" activations that are updated to Android 10. For more information, see the Administration content.</p> |

Android Enterprise provides full support for managing Android devices, including the following features:

- Enforce password requirements
- Control device capabilities using IT policies (for example, disable the camera or Bluetooth)
- Enforce compliance rules
- Create Wi-Fi and VPN connection profiles (with proxy)
- Sync email, contacts, and calendar with devices
- Send CA and client certificates to devices for authentication and S/MIME
- Manage required and allowed public and internal apps
- Locate and protect lost or stolen devices

Android Enterprise devices that are activated with BlackBerry UEM also support additional controls available only for Samsung Knox Platform for Enterprise devices and for BlackBerry devices powered by Android.

BlackBerry UEM also supports devices with Samsung Knox Workspace activations in addition to supporting Samsung Knox Platform for Enterprise; however, Samsung Knox activation types will be deprecated in a future release. For more information, visit <https://support.blackberry.com/community> to read article 54614.

Note: Some features and BlackBerry Dynamics apps are not available with all license levels. For more information about available licenses, see the [Licensing content](#).

Steps to manage Android devices

| Step | Action |
|------|---|
| 1 | Install and configure BlackBerry UEM according to the Installation instructions . |
| 2 | If your organization intends to manage Android Enterprise devices, configure a managed Google Play account or a connection to your Google Cloud or G Suite domain . |
| 3 | Configure IT policies for devices. Assign IT policies to user groups or individual users. |
| 4 | Configure profiles for devices. Assign profiles to to user groups or individual users. |
| 5 | Specify the apps that devices can or must install . |
| 6 | Activate devices. |
| 7 | Manage and monitor devices. |

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 | <p>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.</p> <p>For more information, see Support Android Enterprise activations using managed Google Play accounts</p> |
| G Suite domain | <p>Your organization has a G Suite domain, which supports all G Suite services such as Gmail, Google Calendar, and Google Drive.</p> <p>For more information, see Support Android Enterprise activations with a G Suite domain</p> |
| Google Cloud domain | <p>Your organization has a Google Cloud domain, which provides managed Google accounts to users. Your organization doesn't use G Suite services such as Gmail, Google Calendar, and Google Drive for your organization's email, calendar, and data management.</p> <p>For more information, see Support Android Enterprise activations with a Google Cloud domain</p> |
| No Google services | <p>Your organization's security policies do not allow you to use Google services.</p> <p>For more information, see Support Android Enterprise devices without access to Google Play</p> |

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 G Suite domain

If you have configured BlackBerry UEM to connect to a G Suite 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 G Suite domain, create user accounts for your Android users.
2. Select the **Enforce EMM Policy** setting in the G Suite 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 G Suite 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 G Suite account.
5. Make sure that your users know the passwords for their G Suite 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 | <ul style="list-style-type: none">• 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 | <p>If you want to include the UEM Client location in a QR code, verify the following device activation default settings:</p> <ul style="list-style-type: none">• 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 | <p>Verify the following settings in the activation profile:</p> <ul style="list-style-type: none"> • 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 | <p>For users that are assigned the Work and personal - user privacy (Android Enterprise) activation type, verify the following in the IT policy:</p> <ul style="list-style-type: none"> • 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 | <p>For non-BlackBerry Dynamics apps, add the apps to UEM as internal apps and assign them to users.</p> <ol style="list-style-type: none"> 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 | <p>For BlackBerry Dynamics apps, upload the internal app source file and assign the app to users.</p> <p>Perform the following steps to install or update internal apps on devices that don't have access to Google Play:</p> <ol style="list-style-type: none"> 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.

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 | <p>This setting specifies the types of characters in an automatically generated password. Passwords can include the following types of characters:</p> <ul style="list-style-type: none"> • Lowercase letters • Uppercase letters • Numbers • Special characters or symbols |
| Enable MDM controls activation type for Android devices | <p>This setting specifies whether MDM controls is included in the list of Android activation types in the activation profile.</p> <p>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.</p> <p>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.</p> |
| 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 . |

Controlling Android devices with an IT policy

BlackBerry UEM sends an IT policy to each device. You can use a default IT policy or create your own IT policies. You can create as many IT policies as you require for different situations and different users, but only one IT policy is active on a device at any time.

The IT policy rules for Android are based on the capabilities of the device and the device configuration options provided by Google and the device manufacturer. As Google releases new OS updates with new features and configuration options, new IT policy rules are added to UEM at the next possible opportunity.

You can download the searchable and sortable [IT Policy rule spreadsheet](#). The spreadsheet documents all available rules in UEM, including the minimum device OS that supports the rule.

Device behavior you control with an IT policy includes the following options:

- Device [password requirements](#)
- Allowing device features such as the camera and, Bluetooth
- Allowing apps in one profile to access data in another profile
- Restricting functionality only for apps and data in the work profile.

For more information on sending IT policies to devices, [see the Administration content](#).

Setting Android password requirements

There are four groups of IT policy rules for Android passwords. The group of rules that you use depends on the device activation type and whether you are setting requirements for the device password or the work space password.

After you set password rules in the IT policy, use a [compliance profile](#) to enforce the password requirements.

| Activation type | Supported password rules |
|---|--|
| Work and personal - user privacy (Android Enterprise) and Work and personal - full control (Android Enterprise) | Use the global password rules to set device password requirements. Use the work profile password rules to set the password requirements for the work profile. Knox password rules are ignored by the device. |
| Work space only (Android Enterprise) | Use the global password rules to set password requirements for the device. Because the device only has a work space, the password is also the work space password. All other password rules are ignored by the device. |
| MDM controls | Use the global password rules to set device password requirements. All other password rules are ignored by the device. Note: The MDM controls activation type is deprecated for devices with Android 10. For more information, visit https://support.blackberry.com/community to read article 48386. |

| Activation type | Supported password rules |
|---|--|
| MDM controls (Samsung Knox) | <p>Use the Knox MDM password rules to set device password requirements.</p> <p>All other password rules are ignored by the device.</p> |
| Work and personal - user privacy (Samsung Knox) | <p>You have no control over the device password.</p> <p>Use the Knox Premium - Workspace password rules to set password requirements for the work space.</p> <p>All other password rules are ignored by the device.</p> <p>Note: The 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.</p> |
| Work and personal - full control (Samsung Knox) | <p>Use the Knox MDM password rules to set device password requirements.</p> <p>Use the Knox Premium - Workspace password rules to set password requirements for the work space.</p> <p>All other password rules are ignored by the device.</p> |
| Work space only (Samsung Knox) | <p>Use the Knox Premium - Workspace password rules to set password requirements for the work space.</p> <p>All other password rules are ignored by the device.</p> |

Android: Global password rules

The global password rules set the device password requirements for devices with the following activation types:

- Work and personal - user privacy (Android Enterprise)
- Work and personal - full control (Android Enterprise)
- Work space only (Android Enterprise)
- MDM controls (without Samsung Knox)

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

| Rule | Description |
|--|--|
| Password complexity (Global (all Android devices)) | <p>Specify the minimum complexity level for the device password. You can choose one of the following options:</p> <ul style="list-style-type: none"> • Low - allows patterns and PINs with repeating or sequential values. • Medium - requires PINs with no repeating or sequential values and a minimum length of four or a password with a minimum length of four. • High - requires PINs with no repeating or sequential values and minimum length of eight or a password with a minimum length of six. <p>Note: If you set the password complexity to High, and you then set the password complexity to Medium in the Work profile (all Android devices) section of the IT policy, the global setting takes precedence over the Work profile setting and users will be forced to set a password with high complexity.</p> |
| Password requirements | <p>Specify the minimum requirements for the password. You can choose one of the following options:</p> <ul style="list-style-type: none"> • Unspecified - no password required • Something - the user must set a password but there are no requirements for length or quality • Numeric - the password must include at least one number • Alphabetic - the password must include at least one letter • Alphanumeric - the password must include at least one letter and one number • Complex - allows you to set specific requirements for different character types |
| Password complexity (Work profile (all Android devices)) | <p>Specify the minimum complexity level for the device password. You can choose one of the following options:</p> <ul style="list-style-type: none"> • Low - allows patterns and PINs with repeating or sequential values. • Medium - requires PINs with no repeating or sequential values and a minimum length of four or a password with a minimum length of four. • High - requires PINs with no repeating or sequential values and minimum length of eight or a password with a minimum length of six. <p>Note: If you the password complexity to Medium or low, and you have already set the password complexity to High in the Global (all Android devices) section of the IT policy, the global setting takes precedence over the Work profile setting and users will be forced to set a password with high complexity.</p> |
| Maximum failed password attempts | <p>Specify the number of times that a user can enter an incorrect password before a device is wiped or deactivated.</p> <p>Devices with the "MDM controls" activation type are wiped.</p> <p>Devices with the "Work and personal - user privacy " and the "Work and personal - user privacy (Premium)" activation types are deactivated and the work profile removed.</p> |
| Maximum inactivity time lock | <p>Specify the maximum number of minutes of user inactivity that must elapse before the device or work space locks. On Android devices with a work profile, the work space also locks. Users can set a shorter time period on the device. This rule is ignored if no password is required.</p> |

| Rule | Description |
|--|--|
| Password expiration timeout | Specify the maximum amount of time that the password can be used. After the specified amount of time elapses, the user must set a new password. If set to 0, the password does not expire. |
| Password history restriction | Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a recent numeric, alphabetic, alphanumeric, or complex password. If set to 0, the device does not check previous passwords. |
| Minimum password length | Specify the minimum number of characters for a numeric, alphabetic, alphanumeric, or complex password. |
| Minimum uppercase letters required in password | Specify the minimum number of uppercase letters that a complex password must contain. |
| Minimum lowercase letters required in password | Specify the minimum number of lowercase letters that a complex password must contain. |
| Minimum letters required in password | Specify the minimum number of letters that a complex password must contain. |
| Minimum non-letters in password | Specify the minimum number of non-letter characters (numbers or symbols) that a complex password must contain. |
| Minimum numerical digits required in password | Specify the minimum number of numerals that a complex password must contain. |
| Minimum symbols required in password | Specify the minimum number of non-alphanumeric characters that a complex password must contain. |

For more information about the IT policy password rules, [download the Policy Reference Spreadsheet](#).

Android: Work profile password rules

The work profile password rules set the work space password requirements for devices with the following activation types:

- Work and personal - user privacy (Android Enterprise)
- Work and personal - full control (Android Enterprise)

| Rule | Description |
|--|--|
| Password requirements | <p>Specify the minimum requirements for the work space password. You can choose one of the following options:</p> <ul style="list-style-type: none"> • Something - the user must set a password but there are no requirements for length or quality • Numeric - the password must include at least one number • Alphabetic - the password must include at least one letter • Alphanumeric - the password must include at least one letter and one number • Complex - allows you to set specific requirements for different character types • Numeric Complex - the password must contain numeric characters with no repeating sequence (4444) or ordered sequence (1234, 4321, 2468). • Biometric Weak - the password allows for low-security biometric recognition technology <p>For BlackBerry devices powered by Android, you can force the work space and device passwords to be different using the BlackBerry devices "Force the device and work space passwords to be different" rule.</p> |
| Maximum failed password attempts | Specify the number of times that a user can enter an incorrect work space password before the device is deactivated and the work profile is removed. |
| Maximum inactivity time lock | Specify the maximum number of minutes of user inactivity that must elapse before the device and work space lock. If you set both this rule and the Android global "Maximum inactivity time lock" rule, the device and work space lock when either timer expires. Users can set a shorter time period on the device. |
| Password expiration timeout | Specify the maximum amount of time that the work space password can be used. After the specified amount of time elapses, the user must set a new work space password. If set to 0, the password does not expire. |
| Password history restriction | Specify the maximum number of previous work space passwords that a device checks to prevent a user from reusing a recent numeric, alphabetic, alphanumeric, or complex password. If set to 0, the device does not check previous passwords. |
| Minimum password length | Specify the minimum number of characters for a numeric, alphabetic, alphanumeric, or complex work space password. |
| Minimum uppercase letters required in password | Specify the minimum number of uppercase letters that a complex work space password must contain. |
| Minimum lowercase letters required in password | Specify the minimum number of lowercase letters that a complex work space password must contain. |
| Minimum letters required in password | Specify the minimum number of letters that a complex work space password must contain. |
| Minimum non-letters in password | Specify the minimum number of non-letter characters (numbers or symbols) that a complex work space password must contain. |

| Rule | Description |
|---|---|
| Minimum numerical digits required in password | Specify the minimum number of numerals that a complex work space password must contain. |
| Minimum symbols required in password | Specify the minimum number of non-alphanumeric characters that a complex work space password must contain. |
| Force the device and work profile passwords to be different | Specify whether users must set different passwords for the device and the work profile. When the passwords are the same, unlocking the device unlocks the work profile. |

For more information about the IT policy password rules, [download the Policy Reference Spreadsheet](#).

Controlling Android devices with profiles

BlackBerry UEM includes several profiles that you can use to control various aspects of device functionality. The most commonly used include the following profiles:

| Profile name | Description | Configure |
|----------------------------------|---|---|
| Activation | Specifies the device activation settings for users, such as the activation type, method, and the number and types of devices a user can activate. | Create an activation profile |
| Wi-Fi | Specifies settings for devices to connect to your work Wi-Fi network. | Create a Wi-Fi profile |
| VPN | Specifies settings for devices to connect to a work VPN. | Create a VPN profile |
| Proxy | Specifies how devices use a proxy server to access web services on the Internet or a work network. | Create a proxy profile |
| Email | Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data. If you install and configure BlackBerry Work on devices, you don't need to set up an email profile. | Create an email profile |
| BlackBerry Dynamics | Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. | Create a BlackBerry Dynamics profile |
| BlackBerry Dynamics connectivity | Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when they use BlackBerry Dynamics apps. | Create a BlackBerry Dynamics connectivity profile |
| Compliance | Defines the device conditions that are not acceptable in your organization and sets enforcement actions. | Create a compliance profile |
| Enterprise connectivity | Specifies whether devices can use BlackBerry Secure Connect Plus. | Enable BlackBerry Secure Connect Plus |
| CA certificate | Specifies a CA certificate that devices can use to establish trust with a work network or server. | Create a CA certificate profile |
| User credential | Specifies how devices obtain client certificates used to authenticate with a work network or server. | Create a user credential profile |

| Profile name | Description | Configure |
|--------------|---|---------------------------------------|
| SCEP | Specifies the SCEP server that devices use to obtain a client certificate used to authenticate with a work network or server. | Create a SCEP profile |

For more information on sending profiles to devices, [see the Administration content](#).

Profiles reference - Android devices

The following table lists all BlackBerry UEM profiles supported on Android devices:

| Profile name | Description | Configure |
|--------------------------------------|--|--|
| Policy | | |
| Activation | Specifies the device activation settings for users, such as the activation type and the number and types of devices. | Create an activation profile |
| BlackBerry Dynamics | Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. | Create a BlackBerry Dynamics profile |
| App lock mode | Specify a single app to run on devices. Samsung Knox devices activated with MDM only | Create an app lock mode profile |
| Enterprise Management Agent | Specifies when devices connect to BlackBerry UEM for app or configuration updates when a push notification is not available. | Create an Enterprise Management Agent profile |
| Compliance | | |
| Compliance | Defines the device conditions that are not acceptable in your organization and sets enforcement actions. | Create a compliance profile |
| Compliance (BlackBerry Dynamics) | This is a read-only profile that displays the compliance settings that were imported from Good Control into an on-premises BlackBerry UEM. | Managing BlackBerry Dynamics compliance profiles |
| Device SR requirements | Defines the software release versions that devices must have installed and specifies an update period for apps that are running in the foreground. | Create a device SR requirements profile |
| Email, calendar, and contacts | | |

| Profile name | Description | Configure |
|----------------------------------|--|---|
| Email | Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler. | Create an email profile |
| IMAP/POP3 email | Specifies how devices connect to an IMAP or POP3 mail server, and how to synchronize email messages. | Create an IMAP/POP3 email profile |
| Gatekeeping | Specifies the Microsoft Exchange servers to use for automatic gatekeeping. | Create a gatekeeping profile |
| Networks and connections | | |
| Wi-Fi | Specifies how devices connect to a work Wi-Fi network. | Create a Wi-Fi profile |
| VPN | Specifies how devices connect to a work VPN. | Create a VPN profile |
| Proxy | Specifies how devices use a proxy server to access web services on the Internet or a work network. | Create a proxy profile |
| Enterprise connectivity | Specifies how devices can connect to your organization's resources using enterprise connectivity. For Android Enterprise and Samsung Knox Workspace devices, the enterprise connectivity profile specifies whether devices can use BlackBerry Secure Connect Plus. | Enable BlackBerry Secure Connect Plus |
| BlackBerry Dynamics connectivity | Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps. | Create a BlackBerry Dynamics connectivity profile |
| BlackBerry 2FA | Enables two-factor authentication for users and specifies the configuration of the preauthentication and self-rescue features. | Create a BlackBerry 2FA profile |
| Access Point Name profile | Allows you to specify APNs for devices to use to connect to carriers. | Create an Access Point Name profile |
| Protection | | |
| Microsoft Intune app protection | Allows you to manage apps protected by Microsoft Intune. | Create a Microsoft Intune app protection profile |
| Location service | Allows you to request the location of devices and view the approximate locations on a map. | Create a location service profile |

| Profile name | Description | Configure |
|-----------------------------|---|--|
| Do not disturb | Allows you to block BlackBerry Work for Android notifications during off-work days and hours that you define. | Create a Do not disturb profile |
| Custom | | |
| Device | Allows you to configure the information that displays on devices. | Create a device profile |
| Certificates | | |
| CA certificate | Specifies a CA certificate that devices can use to establish trust with a work network or server. | Create a CA certificate profile |
| Shared certificate | Specifies a client certificate that devices can use to authenticate users with a work network or server. | Create a shared certificate profile |
| User credential | Specifies the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server. | Create a user credential profile |
| SCEP | Specifies the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server. | Create a SCEP profile |
| CRL | Specifies the CRL configurations that BlackBerry UEM can use to check the status of certificates. BlackBerry devices powered by Android only | Create a CRL profile |
| Certificate mapping profile | Specifies which client certificates apps must use | Create a certificate mapping profile |

Managing apps on Android devices

You can create a library of apps that you want to manage and monitor on devices. For Android Enterprise devices, only apps that you allow can be installed to the work profile. BlackBerry UEM provides the following options for managing apps on Android devices:

- [Assign public apps](#) from Google Play as optional or required on devices.
- [Upload custom apps](#) to UEM and deploy them as optional or required apps.
- [Preconfigure app settings](#), such as connection settings, when allowed by the app.
- [Block users from accessing apps](#).
- [Configure public, ISV, and custom BlackBerry Dynamics apps](#) to allow users to access work resources.
- [Connect UEM to Microsoft Intune](#) to set Intune app protection policies from within the UEM management console to deploy and manage Office 365 apps.
- [View the list of personal apps installed on devices](#).
- [Allow users to rate and review apps](#) for other users in your environment.

App behavior on Android Enterprise devices

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

For Android Enterprise devices, the following behavior occurs:

| App type | When the app is assigned to a user | When apps are updated | When the app is unassigned from a user | When the device is removed from BlackBerry UEM |
|--|--|--|--|--|
| Public apps with a required disposition | Apps are automatically installed. | Apps are automatically updated. | Apps are not automatically removed from the device. Apps are grayed out on the device and must be removed manually. | The work profile and assigned work apps are removed from the device. |
| Public apps with an optional disposition | The user can choose whether to install the apps. Apps appear in Google Play for Work. | Google Play for Work notifies users about updates. | Apps are not automatically removed from the device. Apps are grayed out on the device and must be removed manually. | The work profile and assigned work apps are removed from the device. |

| App type | When the app is assigned to a user | When apps are updated | When the app is unassigned from a user | When the device is removed from BlackBerry UEM |
|---|--|--|--|--|
| Internal apps with a required disposition hosted in BlackBerry UEM | Supported only for Work space only devices. Apps are automatically installed. | Supported only for Work space only devices. Apps are automatically installed. | Apps are automatically removed from the device. | Apps are automatically removed from the device. |
| Internal apps with an optional disposition hosted in BlackBerry UEM | The user can choose whether to install the apps. Apps appear in Google Play for Work. | Google Play for Work notifies users about updates. | Apps are not automatically removed from the device. Apps are grayed out on the device and must be removed manually. | The work profile and assigned work apps are removed from the device. |
| Internal apps with a required disposition hosted in Google Play | Apps are automatically installed on the device. | Google Play for Work notifies users about updates. | Apps are not automatically removed from the device. Apps are grayed out on the device and must be removed manually. Apps are grayed out on the device and must be removed manually. | The work profile and assigned work apps are removed from the device. |
| Internal apps with an optional disposition hosted in Google Play | The user can choose whether to install the apps. Apps appear in Google Play for Work. | Google Play for Work notifies users about updates. | Apps are not automatically removed from the device. Apps are grayed out on the device and must be removed manually. | The work profile and assigned work apps are removed from the device. |

You can specify update behavior for apps running the the foreground in the [device SR requirements profile](#).

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 | <p>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.</p> <p>For more information, see Activate an Android Enterprise device with the Work and personal - user privacy activation type.</p> |
| User downloads the UEM Client from the BlackBerry download site | <p>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.</p> <p>For more information, visit support.blackberry.com/community to read article 42607.</p> |
| Enter Google domain credentials during device setup | <p>If BlackBerry UEM is connected to your organization's G Suite 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.</p> <p>For more information, see Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain.</p> |
| Scan a QR Code that contains the UEM Client download location | <p>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.</p> <p>Some device manufacturers may not support this functionality.</p> <p>For more information, see Activate an Android Enterprise device with the Work and personal - full control activation type using a managed Google Play account.</p> |

| Activation method | Description |
|--|---|
| Enter the <code>afw#blackberry</code> hashtag during device setup | <p>If your organization uses managed Google Play accounts to connect to Google services, to activate devices that are assigned the Work space only or Work and personal - full control activation type, on the screen where users enter their Google credentials during device setup, they can instead type <code>afw#blackberry</code> to initiate downloading the UEM Client and begin the activation process.</p> <p>For Android 11 and later devices, <code>afw#blackberry</code> is supported only for the Work space only activation type.</p> <p>For Android 8 and 9 devices, <code>afw#blackberry</code> is no longer supported.</p> <p>For more information, see Activate an Android Enterprise device with the Work space only activation type using a managed Google Play account.</p> |
| Tap an NFC sticker or a secondary device with the BlackBerry UEM Enroll app that is programmed with the UEM Client download location | <p>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.</p> <p>The same secondary device or NFC sticker can be used to activate devices for multiple users.</p> <p>For more information, see Activate an Android Enterprise device without access to Google Play.</p> |
| Android zero-touch enrollment or Samsung Knox Mobile Enrollment | <p>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.</p> <p>For more information see Configure support for Android zero-touch enrollment or Activate multiple devices using Knox Mobile Enrollment.</p> |

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 |

| 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 |
| Google domain credentials | Yes | Yes | No | No | Yes | No | No |
| Scan QR Code | No | Yes | Yes | Yes | Yes | Yes | Yes |
| afw#blackberry hashtag | No | No | Android 10 | No | No | Android 10 and later | No |
| 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 |

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) | <p>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.</p> <p>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.</p> <p>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.</p> <p>Users do not have to grant Administrator permissions to the BlackBerry UEM Client.</p> |
| Work and personal - full control (Android Enterprise fully managed device with work profile) | <p>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).</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>To specify whether BlackBerry UEM can limit activation by device ID, select Allow only approved device IDs.</p> <p>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.</p> <p>During activation users must grant Administrator permissions to the BlackBerry UEM Client.</p> |

| Activation type | Description |
|--|--|
| Work space only (Android Enterprise fully managed device) | <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>To specify whether BlackBerry UEM can limit activation by device ID, select Allow only approved device IDs.</p> <p>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.</p> |

Android devices without a work profile

The following activation types apply to all Android devices.

| Activation type | Description |
|---|--|
| MDM controls | <p>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.</p> <p>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.</p> <p>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.</p> <p>During activation, users must grant Administrator permissions to the BlackBerry UEM Client.</p> |
| User privacy | <p>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.</p> <p>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.</p> |
| Device registration for BlackBerry 2FA only | <p>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.</p> <p>When a device is activated, you can view limited device information in the management console, and you can deactivate the device using a command.</p> <p>This activation type is supported only for Microsoft Active Directory users.</p> <p>For more information, see the BlackBerry 2FA content.</p> |

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) | <p>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.</p> <p>During activation, users must grant Administrator permissions to the BlackBerry UEM Client.</p> |
| Work and personal - full control (Samsung Knox) | <p>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).</p> <p>During activation users must grant Administrator permissions to the BlackBerry UEM Client.</p> |
| Work space only - (Samsung Knox) | <p>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.</p> <p>During activation, users must grant Administrator permissions to the BlackBerry UEM Client.</p> |

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 Compatibility 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 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 by "Work space only" and "Work and personal - full control" devices.
- e) In the **SafetyNet attestation options** section, optionally select one of the following attestation methods:
- **Perform SafetyNet attestation for device:** Use this method to send challenges to test the authenticity and integrity of devices.
 - **Perform SafetyNet attestation on device activation:** Use this method to send challenges to test the authenticity and integrity of devices when they are activated.
 - **Perform SafetyNet 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.

11. Click **Add**.

After you finish: If necessary, rank profiles.

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)**.

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 | <p>To support Knox DualDAR encryption, create an activation profile with the following settings for Android devices:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> |
| BlackBerry UEM Client | A version of BlackBerry UEM Client for Android later than 12.35.2.155980 is required. |

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 | <ol style="list-style-type: none">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 | <ol style="list-style-type: none">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 G Suite 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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 space only 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](#).


These instructions also work for Android 10 devices with the Work and personal - full control activation type.

For Android 8 and 9 devices, see [Activate an Android Enterprise device with the Work and personal - full control activation type using a managed Google Play account](#) instead. Android 8 and 9 devices no longer support the afw#blackberry hashtag to initiate Work space only or Work and personal - full control activations.

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 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 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, type afw#blackberry in the Google account login screen.
 3. 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 | <ol style="list-style-type: none"> Tap . Tap Allow to allow the UEM Client to take pictures and record video. Scan the QR Code in the activation email message that you received. |
| Manually activate the device | <ol style="list-style-type: none"> Type your work email address. Tap Next. Type your activation password. Tap Activate My Device. 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. If necessary, type your username and activation password. Tap Next. |

- Wait while the profiles and settings are pushed to your device.
- On the **Set up your profile** screen, tap **Set up** and wait while a work profile is set up on the device.
- If you are prompted, log in to your Google account with your Google email address and password.
- On the unlock selection screen, choose a screen unlock method.
- If you are prompted with the **Secure start-up** screen, tap **Yes** to require a password when the device starts.
- Type a device password and type it again to confirm it. Tap **OK**.
- Select one of the options for how you want your notifications to show. Tap **Done**.
- 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.
- 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**.
- If you are signed out of your device, unlock your device to complete the BlackBerry UEM activation.
- If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
- 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 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)
 - Your 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 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 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. 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 | <ol style="list-style-type: none"> a. Tap . b. Tap Allow to allow the UEM Client to take pictures and record video. |


| Task | Steps |
|---|--|
| | 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 . |

Task

Steps

- 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.

Managing and monitoring activated Android devices

After devices are activated and managed by an IT policy and profiles, you have several features available to control users' devices.

You have the following options:

| Option | Description |
|---|--|
| Control which software updates are installed on devices and the timing of updates | <p>You can use a the device SR requirements profile to specify if and when OS updates are installed on the following devices:</p> <ul style="list-style-type: none">• Android Enterprise devices that have a Work space only activation• Samsung Knox devices <p>For more information, see the Administration content</p> <p>You can use Compliance profiles to specify restricted OS versions. For more information, see the Administration content.</p> |
| Turn on location settings and locate a device | <p>You can turn on location settings to track the location of Android devices.</p> <p>For more information, see the Administration content.</p> |
| Retrieve device logs | <p>You can retrieve logs from devices for monitoring and troubleshooting purposes.</p> <p>For more information, see the Administration content.</p> |
| Deactivate a device | <p>When you or a user deactivates a device, the connection between the device and the user account in BlackBerry UEM is removed. You can't manage the device and the device is no longer displayed in the management console. The user can't access work data on the device.</p> <p>You can deactivate a device using the "Delete all device data" or "Delete only work data" command.</p> <p>Users can deactivate an Android device by selecting Deactivate My Device on the About screen in the BlackBerry UEM Client app.</p> |

Commands for Android devices

| Command | Description | Activation types |
|---------------------|--|-----------------------------|
| View device report | This command displays detailed information about a device. You can export and save the device report on your computer. For more information, see View and save a device report . | All (except BlackBerry 2FA) |
| View device actions | This command displays any actions that are in progress on a device. For more information, see Viewing device actions . | All (except BlackBerry 2FA) |

| Command | Description | Activation types |
|------------------------|---|---|
| Lock device | <p>This command locks the device. The user must type the existing device password to unlock the device. If a device is temporarily lost, you might use this command.</p> <p>When you send this command, the device locks only if there is an existing device password. Otherwise, no action is taken on the device.</p> | <p>MDM controls</p> <p>Work and personal - full control (Android Enterprise)</p> <p>Work and personal - user privacy (Android Enterprise)</p> <p>Work space only (Android Enterprise)</p> |
| Delete all device data | <p>This command deletes all user information and app data that the device stores, including information in the work space and returns the device to factory default settings.</p> <p>If the device is unable to connect to BlackBerry UEM when you send this command, you can either cancel the command or remove the device from the console. If the device connects to BlackBerry UEM after you remove it, only the work data is deleted from the device, including the work space, if applicable.</p> <p>To send this command to multiple devices, see Send a bulk command.</p> | <p>MDM controls</p> <p>Work and personal - full control (Android Enterprise)</p> <p>Work and personal - full control (Samsung Knox)</p> <p>Work space only - (Samsung Knox)</p> |
| Delete only work data | <p>This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device and deactivates the device. If the device has a work space, the work space information and the work space are deleted from the device but all personal apps and data remain on the device. For more information, see Deactivating devices.</p> <p>When you use this command on Android Enterprise devices, you can type a reason that appears in the notification on the user's device to explain why the work profile was deleted.</p> <p>For Work and personal - full control (Android Enterprise) activations, this command is supported only by devices running Android 11 and later.</p> <p>If the device is unable to connect to BlackBerry UEM when you send this command, you can either cancel the command or remove the device from the console. If the device connects to BlackBerry UEM after you remove it, the work data is deleted from the device, including the work space, if applicable.</p> <p>To send this command to multiple devices, see Send a bulk command.</p> | <p>MDM controls</p> <p>Work and personal - user privacy (Android Enterprise)</p> <p>Work and personal - full control (Android Enterprise)</p> <p>Work and personal - user privacy (Samsung Knox)</p> <p>Work and personal - full control (Samsung Knox)</p> <p>Work space only - (Samsung Knox)</p> |

| Command | Description | Activation types |
|--------------------------------------|--|--|
| Unlock device and clear password | <p>This command unlocks the device and prompts the user to create a new device password. If the user skips the "Create device password" screen, the previous password is retained. You can use this command if a user forgets the device password.</p> <p>Note: This command is not supported by devices with Samsung Knox SDK 3.2.1 and later.</p> | <p>MDM controls (Samsung devices only)</p> <p>Work and personal - full control (Samsung Knox)</p> <p>Work and personal - user privacy (Samsung Knox)</p> |
| Specify device password and lock | <p>This command lets you create a device password and then lock the device. You must create a password that complies with existing password rules. To unlock the device, the user must type the new password.</p> <p>Note: For the Work and personal - user privacy activation types, only BlackBerry devices powered by Android 8.x and later support this command.</p> <p>Note: For the Work and personal - full control (Android Enterprise) activation type, only devices that use a version of the Android OS earlier than Android 11 support this command.</p> | <p>Work and personal - full control (Samsung Knox)</p> <p>Work space only (Android Enterprise)</p> <p>Work and personal - full control (Android Enterprise)</p> <p>Work and personal - user privacy (Android Enterprise)</p> |
| Reset work space password | <p>This command deletes the current work space password from the device. When the user opens the work space, the device prompts the user to set a new work space password.</p> | <p>Work and personal - full control (Samsung Knox)</p> <p>Work and personal - user privacy - (Samsung Knox)</p> <p>Work space only - (Samsung Knox)</p> |
| Specify work space password and lock | <p>You can specify a work profile password and lock the device. When the user opens a work app, they must type the password that you specified.</p> | <p>Work and personal - user privacy (Android Enterprise)</p> <p>Work and personal - full control (Android Enterprise)</p> |
| Disable/enable work space | <p>This command disables or enables access to the work space apps on the device.</p> | <p>Work and personal - full control (Samsung Knox)</p> <p>Work and personal - user privacy - (Samsung Knox)</p> <p>Work space only - (Samsung Knox)</p> |
| Deactivate BlackBerry 2FA | <p>This command deactivates devices that are activated with the BlackBerry 2FA activation type. The device is removed from BlackBerry UEM and the user can't use the BlackBerry 2FA feature.</p> | <p>BlackBerry 2FA</p> |

| Command | Description | Activation types |
|---------------------------|--|--|
| Wipe apps | <p>This command wipes data from all Microsoft Intune-managed apps on the device. The apps are not removed from the device.</p> <p>For more information, see Wipe apps managed by Microsoft Intune</p> | All (except BlackBerry 2FA) |
| Update device information | <p>This command sends and receives updated device information. For example, you can send newly updated IT policy rules or profiles to a device, and receive updated information about a device such as OS version or battery level.</p> <p>To send this command to multiple devices, see Send a bulk command.</p> | All (except BlackBerry 2FA) |
| Request bug report | This command sends a request to the device for the client logs. The device user must accept or decline the request. | <p>Work space only (Android Enterprise)</p> <p>Work and personal - full control (Android Enterprise)</p> |
| Restart device | This command sends a request to the device to restart. A message displays to the user that the device will restart in one minute. The device user has the option to snooze the restart for 10 minutes. | Work space only (Android Enterprise) |
| Remove device | <p>This command removes the device from BlackBerry UEM but does not remove data from the device. The device may continue to receive email and other work data.</p> <p>This command is intended for devices that have been irretrievably lost or damaged and are not expected to contact the server again. If a device that has been removed attempts to contact BlackBerry UEM, the user receives a notification and the device won't be able to communicate with BlackBerry UEM unless it is reactivated.</p> <p>To send this command to multiple devices, see Send a bulk command.</p> | All (except BlackBerry 2FA) |

Enable users to unlock a BlackBerry Dynamics app using a third-party identity provider

You can enable your users to unlock or restore a BlackBerry Dynamics app using your identity provider, such as Ping Identity or Okta.

Before you begin: Verify that you have set up your organization's third-party identity provider. For more information, see the BlackBerry Enterprise Identity [administration content](#).

1. In the BlackBerry UEM management console, navigate to **Settings > User Roles**.
2. Select the **Lock and unlock BlackBerry Dynamics apps** option.

Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at <http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp>.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

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

Published in Canada