BlackBerry UEM

Managing Android devices

Administration

12.11

Contents

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. For more information, see Activate a device using a QR Code.

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	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. 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.
Managed devices with a work profile Work and personal - user privacy (Android Enterprise) activations	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. 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.
Fully managed devices with a work profile Work and personal - full control (Android Enterprise) activations	Android Enterprise 8.0 and later 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. You can log SMS, MMS, and phone calls sent and received on the device. Work and personal data are both protected using encryption and password authentication. This option is often used for COPE devices.
Fully managed devices Work space only (Android Enterprise) activations	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. 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.

Control level	Description
Device administration MDM controls activations	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. This activation type is deprecated for Android 10 devices. For more information, visit https://support.blackberry.com/community to read article 48386. 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.

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.

Licenses consumed by Android devices

When you or a user activates an Android device with BlackBerry UEM, you associate the device with BlackBerry UEM so that you can manage devices and users can access work data on their devices. Some Android activation types require a minimum of a Silver BlackBerry UEM license or a BlackBerry Enterprise Mobility Suite - Management Edition license, but other licenses may be required depending on the features that you want to enable for users.

Feature	Minimum Required license
MDM controls, User privacy activation, or Android Enterprise activation	One of the following: • Silver • BlackBerry Enterprise Mobility Suite - Management Edition
Samsung KNOX Workspace activation	One of the following: • Gold Cross-Platform • Gold - KNOX Workspace • BlackBerry Enterprise Mobility Suite - Collaboration Edition
BlackBerry Secure Connect Plus	One of the following: • Gold • BlackBerry Enterprise Mobility Suite - Collaboration Edition For more information about BlackBerry Secure Connect Plus, see the BlackBerry UEM Administration content or the BlackBerry UEM Cloud Administration content.
BlackBerry Access app	BlackBerry Enterprise Mobility Suite - Management Edition
BlackBerry Work and BlackBerry Tasks apps	BlackBerry Enterprise Mobility Suite - Enterprise Edition
All other BlackBerry and ISV BlackBerry Dynamics apps	BlackBerry Enterprise Mobility Suite - Collaboration Edition
Device registration for BlackBerry 2FA only	One of the following: • BlackBerry 2FA • BlackBerry Enterprise Mobility Suite - Application Edition

For more information about 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	Verify that you have the required licenses to activate Android devices with the features that you want to enable.
4	Configure IT policies for devices. Assign IT policies to user groups or individual users.
5	Configure profiles for devices. Assign profiles to to user groups or individual users.
6	Specify the apps that devices can or must install.
7	Activate devices.
8	Manage and monitor devices.

Supporting Android Enterprise activations

Organizations that use Android Enterprise devices have several options for connecting to Google services. How your organization uses Google services determines how you connect BlackBerry UEM to Google services and how you activate devices. For more information on configuring BlackBerry UEM to connect to a Google domain or use managed Google Play accounts, see the Configuration content.

Your organization may interact with Google services in the following ways:

Google services connection	Description	More information
Managed Google Play accounts	BlackBerry UEM is not connected to a Google domain. You can use managed Google Play accounts to allow users to download and install work apps using Google Play.	Support Android Enterprise activations using managed Google Play accounts Activate an Android Enterprise device with the Work and personal - user privacy activation type Activate an Android Enterprise device using a managed Google Play account
G Suite domain	Your organization has a G Suite domain, which supports all G Suite services such as Gmail, Google Calendar, and Google Drive.	Support Android Enterprise activations with a G Suite domain Activate an Android Enterprise device with the Work and personal - user privacy activation type Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain
Google Cloud domain	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.	Support Android Enterprise activations with a Google Cloud domain Activate an Android Enterprise device with the Work and personal - user privacy activation type Activate an Android Enterprise device when BlackBerry UEM is connected to a Google domain
No Google services	Your organization's security policies do not allow you to use Google services.	Support Android Enterprise devices without access to Google Play Activate an Android Enterprise device without a Google Play account

If you support Android Enterprise activations, you can provide users with BlackBerry Hub which allows them to manage both work and personal email messages and calendar data in a unified view. For more information, see Enable a unified BlackBerry Hub.

Support Android Enterprise activations using managed Google Play accounts

If you don't have or don't want to connect BlackBerry UEM to a Google domain, you can activate Android Enterprise devices to use managed Google Play accounts. When you use managed Google Play accounts you can use any Google or Gmail account to connect BlackBerry UEM to Google and no personally identifiable information about your users is sent to Google. For more information on managed Google Play accounts, see https://support.google.com/googleplay/work/.

Once you have connected 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 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 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 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 (for example, due to local restrictions) with UEM, you must install the latest BlackBerry UEM Client on the device that you want to activate. The method that you use to download the UEM Client depends on the activation type:

- **Work space only (Android Enterprise) and Work and personal - full control (Android Enterprise)**: You must manually download the BlackBerry UEM Enroll app from BlackBerry and install it on a secondary device. The device that you want to activate must be reset to default factory settings and, before you complete the out-of-box device setup on the device, you use the UEM Enroll app on the secondary device to download the UEM Client using NFC.
- **Work and personal - user privacy (Android Enterprise)**: After the out-of-box device setup is completed on the device that you want to activate, you must manually download the UEM Client from BlackBerry and install it.

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

Requirements

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

Requirement	Description
BlackBerry UEM environment	Verify the following: • BlackBerry UEM server version 12.11 or later • **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.

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

Requirement	Description
BlackBerry Dynamics apps	For BlackBerry Dynamics apps, upload the internal app source file and assign the app to users.
	Perform the following steps to install or update internal apps on devices that don't have access to Google Play:
	1. Obtain the .apk files of the BlackBerry Dynamics apps that you want to assign. For example, to download BlackBerry Work, visit support.blackberry.com/community and read article 42607.
	2. In the BlackBerry UEM management console, on the menu bar, click **Apps**.
	3. Click a BlackBerry Dynamics app (for example, BlackBerry Work).
	4. Click the **Android** tab.
	5. Click **Add internal app source file**.
	6. Click **Browse** and select the .apk file.
	7. Click **Add**.
	8. Click **Save**.
	9. Repeat the previous steps for each app that you want to add.
	10. Assign the apps to users. The app disposition must be set to **Required**.
Activating the devices	For devices assigned the Work space only (Android Enterprise) and Work and personal - full control (Android Enterprise) activation types, use the UEM Enroll app to initiate the download of the UEM Client. For more information, see the BlackBerry UEM Enroll documentation.
	For devices assigned the Work and personal - user privacy (Android Enterprise) activation type, manually download and install the UEM Client app. For more information, visit support.blackberry.com/community and read article 42607.
	Note:
	• The device on which you install UEM Enroll must be running Android 9 or earlier.
	• The device that you want to activate must be running Android 9 or earlier.
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.

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 the capabilities of the device and the device configuration options provided by Apple. As Apple 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.

Activation type	Supported password rules
MDM controls	Use the global password rules to set device password requirements.
	All other password rules are ignored by the device.
	Use a compliance profile to enforce the password requirements.
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.
	Use a compliance profile to enforce the password requirements.
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.
	For BlackBerry devices powered by Android, you can force the work profile and device passwords to be different.
	All other password rules are ignored by the device.
	Use a compliance profile to enforce the password requirements.

Activation type	Supported password rules
MDM controls (KNOX MDM)	Use the KNOX MDM password rules to set device password requirements. All other password rules are ignored by the device. Use a compliance profile to enforce the password requirements.
Work space only (Samsung KNOX)	Use the KNOX Premium - Workspace password rules to set password requirements for the work space. All other password rules are ignored by the device. Use a compliance profile to enforce the password requirements.
Work and personal - full control (Samsung KNOX)	Use the KNOX MDM password rules to set device password requirements. Use the KNOX Premium - Workspace password rules to set password requirements for the work space. All other password rules are ignored by the device. Use a compliance profile to enforce the password requirements.
Work and personal - user privacy (Samsung KNOX)	You have no control over the device password. Use the KNOX Premium - Workspace password rules to set password requirements for the work space. All other password rules are ignored by the device. Use a compliance profile to enforce the password requirements.

Android: Global password rules

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

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

Rule	Description
Password requirements	Specify the minimum requirements for the password. You can choose one of the following options: • 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

Rule	Description
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped or deactivated.
	Devices with the "MDM controls" activation type are wiped.
	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.
Maximum inactivity time lock	Specify the number of minutes of user inactivity that must elapse before the device or work space locks. This rule is ignored if no password is required.
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 rules 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 - full control (Android Enterprise)

- Work and personal - user privacy (Android Enterprise)

Rule	Description
Password requirements	Specify the minimum requirements for the work space password. You can choose one of the following options: • 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 • 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 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.
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 number of minutes of user inactivity that must elapse before the device and work space lock. If you set both this rule and the Native OS "Maximum inactivity time lock" rule, the device and work space lock when either timer expires.
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.

Rule	Description
Minimum non-letters in password	Specify the minimum number of non-letter characters (numbers or symbols) that a complex work space password must contain.
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.

For more information about the IT policy rules 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 certficate 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. BlackBerry UEM includes a Default compliance profile.	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Control.	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. Enterprise connectivity is always enabled for BlackBerry 10 devices. For BlackBerry 10, Samsung KNOX Workspace, devices, and for iOS devices with MDM controls, the enterprise connectivity profile specifies whether devices can use BlackBerry Secure Connect Plus. BlackBerry UEM includes a Default enterprise connectivity profile.	Create an enterprise connectivity profile
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
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 certficate 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 added it to the BlackBerry Dynamics Launcher.

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

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

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

Activating Android devices

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

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 (Android Enterprise)" first and "MDM controls" second, devices that support Android Enterprise receive the first activation type.

The Android activation types are organized in the following tables:

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

Android Enterprise devices

The following activation types apply only to Android Enterprise devices.

Activation type	Description
Work and personal - user privacy (Android Enterprise with work profile)	This activation type maintains privacy for personal data but lets you manage work data using commands and IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication.
	To allow Google Play app management for Android Enterprise devices, select **Add Google Play to the workspace**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process.
	To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** option.
	Users do not have to grant Administrator permissions to the BlackBerry UEM Client.

Activation type	Description
Work and personal - full control (Android Enterprise fully managed device with work profile)	This activation type lets you manage the entire device using commands and IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files.
	To allow Google Play app management for Android Enterprise devices, select **Add Google Play to the workspace**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process.
	To enable BlackBerry Secure Connect Plus and Knox Platform for Enterprise support, you must select the **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** option.
	During activation users must grant Administrator permissions to the BlackBerry UEM Client.
	This activation type is supported only for Android 8.0 and later.
Work space only (Android Enterprise fully managed device)	This activation type lets you manage the entire device using commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating. The activation process installs a work profile and no personal profile. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password.
	To allow Google Play app management for Android Enterprise devices, select **Add Google Play to the workspace**. This setting is enabled by default. If the device does not have access to Google Play, then this setting must be deselected and the BlackBerry UEM Enroll app must be used from a secondary device during the activation process.
	During activation, the device installs the BlackBerry UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app.
	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.

Android devices without a work profile

The following activation types apply to all Android devices.

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

Samsung KNOX Workspace devices

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

Note: Samsung KNOX activation types will be deprecated in a future release. Devices that support Knox Platform for Enterprise can be activated using the Android Enterprise activation types. For more information, visit https://support.blackberry.com/community to read article 54614.

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

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

Send these activation instructions to users activating devices with the Work and personal - user privacy (Android Enterprise) activation type. The activation steps are the same whether you are using managed Google Play accounts or you are connected to a Google domain.

Before you begin:

- You need the following information:
  - BlackBerry UEM activation password
  - Your work email and password
- You might need the following information:
  - BlackBerry UEM server address
  - Google account password

1. On the device, install the BlackBerry UEM Client. You can download the UEM Client from Google Play.
2. On the device, tap **UEM Client**.
3. Read the license agreement. Tap **I Agree**.
4. Tap **Allow** to allow UEM Client to make and manage phone calls.
5. Type your work email address. Tap **Next**.
6. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
7. Type your activation password. Tap **Activate My Device**.
8. Wait while the profiles and settings are pushed to your device.
9. Tap **Accept & continue** to create a work profile on the device.
10. If necessary, type your Google password. Tap **Next**.
11. If prompted, you can set up a device password and select notification options.
12. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.

Activate an Android Enterprise device using a managed Google Play account

These steps apply to devices that are assigned the Work space only (Android Enterprise) or Work and personal - full control (Android Enterprise) activation type. If users are activating Work and personal - user privacy devices, send them instructions to Activate an Android Enterprise device with the Work and personal - user privacy activation type.

Send the following activation instructions to the device user.

Before you begin: Make sure you have the following information that was sent by your administrator in one or more email messages:

- Activation username
- BlackBerry UEM activation password

1. If you do not see the device setup Welcome screen, reset your device to the factory default setting.
2. During the device setup, in the **Add your account** screen, type afw#blackberry.
3. On the device, tap **Install** to install the BlackBerry UEM Client.
4. Read the license agreement. Tap **I Agree**.
5. Tap **Allow** to allow UEM Client to make and manage phone calls.
6. Type your work email address. Tap **Next**.
7. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
8. Type your activation password. Tap **Activate My Device**.
9. Wait while the profiles and settings are pushed to your device.
10. On the **Set up your device** screen, tap **Accept & Continue** and wait while the work profile is set up.
11. On the **Unlock selection** screen, choose an unlock method.
12. On the **Secure start-up** screen tap **Yes** to require a password when the device starts.
13. Type a device password, type it again to confirm it. Tap **OK**.
14. Select one of the options for how you want your notifications to show. Tap **Done**.

15. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.

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. If users are activating Work and personal - user privacy devices, send them instructions to Activate an Android Enterprise device with the Work and personal - user privacy activation type.

Send the following activation instructions to the device user.

Before you begin: Make sure you have the following information that was sent by your administrator in one or more email messages:

- BlackBerry UEM activation password
- Your work email and password
- BlackBerry UEM server address (you might not need this)

1. If you do not see the device setup Welcome screen, reset your device to the factory default setting.
2. During the device setup, in the **Add your account** screen, enter your work email address and password
3. If you are prompted, encrypt the device.
4. On the device, tap **Install** to install the BlackBerry UEM Client.
5. Read the license agreement. Tap **I Agree**.
6. Tap **Allow** to allow UEM Client to make and manage phone calls.
7. Type your work email address. Tap **Next**.
8. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
9. Type your activation password. Tap **Activate My Device**.
10. Wait while the profiles and settings are pushed to your device.
11. On the **Set up your device** screen, tap **Accept & Continue** and wait while the work profile is set up.
12. On the **Unlock selection** screen, choose an unlock method.
13. On the **Secure start-up** screen tap **Yes** to require a password when the device starts.
14. Type a device password, type it again to confirm it. Tap **OK**.
15. Select one of the options for how you want your notifications to show. Tap **Done**.
16. If prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.

Activate an Android Enterprise device without a Google Play account

These steps apply to devices that do not have access to Google Play. The devices may be assigned the Work space only (Android Enterprise), Work and personal - full control (Android Enterprise), or Work and personal - user privacy (Android Enterprise) activation type.

A secondary device that has the BlackBerry UEM Enroll app installed is required. The same device can be used to help activate an unlimited number of devices with UEM.

Send the following activation instructions to the device user.

Before you begin:

- Make sure you have the following information that was sent by your administrator in one or more email messages:
  - Activation username
  - BlackBerry UEM activation password
- You must have a secondary device that has the BlackBerry UEM Enroll app installed. To download and install the app on a secondary device, visit support.blackberry.com/community to read article 42607.

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 setting.
2. On the secondary device, open the BlackBerry UEM Enroll app. Make sure that NFC is enabled on the device.
3. Tap **Activate device**.
4. Tap the backs of both devices together.
5. On the device that you want to activate, follow the instructions on the screen to download and install the BlackBerry UEM Client.
6. Read the license agreement. Tap **I Agree**.
7. Tap **Allow** to allow UEM Client to make and manage phone calls.
8. Type your work email address. Tap **Next**.
9. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
10. Type your activation password. Tap **Activate My Device**.
11. Wait while the profiles and settings are pushed to your device.
12. On the **Set up your device** screen, tap **Accept & Continue** and wait while the work profile is set up.
13. On the **Unlock selection** screen, choose an unlock method.
14. On the **Secure start-up** screen tap **Yes** to require a password when the device starts.
15. Type a device password, type it again to confirm it. Tap **OK**.
16. Select one of the options for how you want your notifications to show. Tap **Done**.
17. If you are prompted, tap **OK** to allow the connection to BlackBerry Secure Connect Plus and wait while the connection is turned on.
18. If necessary, open the email app that your organization wants you to use (for example, BlackBerry Hub) 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 assigned the MDM controls activation type. 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.

Send the following activation instructions to the device user.

1. On the device, install the BlackBerry UEM Client. You can download the BlackBerry UEM Client from Google Play.
2. On the device, tap **UEM Client**.
3. Read the license agreement. Tap **I Agree**.
4. Type your work email address. Tap **Next**.

5. If necessary, type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.

6. Type your activation password. Tap **Activate My Device**.

7. Tap **Next**.

8. Tap **Activate**.

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

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

Activate a device using a QR Code

QR Code activation is supported on iOS and Android devices.

To activate devices using a QR Code, send the following instructions to the device user.

Before you begin: You need a QR Code. You can find it in the activation email that you received from your administrator, or you can generate one in BlackBerry UEM Self-Service.

1. On the device, install the BlackBerry UEM Client app. For iOS devices, download the app from the App Store. For Android devices, download the app from Google Play.

2. On the device, tap **UEM Client**.

3. Read the license agreement and tap **I Agree**.

4. Scan the QR Code that you received in the activation email or that you generated in BlackBerry UEM Self-Service.

5. If you are prompted to enter the password for your email account or the passcode for your device, follow the instructions on the screen.

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

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

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	You can use a the device SR requirements profile to specify if and when OS updates are installed on the following devices: • Android Enterprise devices that have a Work space only activation • Samsung KNOX devices For more information, see the Administration content You can use Compliance profiles to specify restricted OS versions. For more information, see the Administration content.
Turn on location settings and locate a device	You can turn on location settings to track the location of Android devices. For more information, see the Administration content.
Retrieve device logs	You can retrieve logs from devices for monitoring and troubleshooting purposes. For more information, see the Administration content.
Deactivate a device	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. You can deactivate a device using the "Delete all device data" or "Delete only work data" command. Users can deactivate an Android device by selecting Deactivate My Device on the About screen in the BlackBerry UEM Client app.

Commands for Android devices

Command	Description	Activation types
Delete all device data	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. 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. To send this command to multiple devices, see Send a bulk command.	MDM controls Work and personal - full control (Android Enterprise) Work and personal - full control (Samsung KNOX) Work space only - (Samsung KNOX)
Delete only work data	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. For more information, see Deactivating devices. 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. To send this command to multiple devices, see Send a bulk command.	All (except BlackBerry 2FA)
Lock device	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. When you send this command, the device locks only if there is an existing device password. Otherwise, no action is taken on the device.	MDM controls Work and personal - full control (Samsung KNOX) Work and personal - full control (Android Enterprise) Work and personal - user privacy (Android Enterprise) Work space only (Android Enterprise)

Command	Description	Activation types
Unlock device and clear password	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. **Note:** This command is not supported on non-Samsung devices running Android 7.0 and later that are activated with MDM controls.	MDM controls Work and personal - full control (Samsung KNOX) Work and personal - user privacy (Samsung KNOX)
Specify device password and lock	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. **Note:** This command is not supported on non-Samsung devices running Android 7.0 and later that are activated with MDM controls. **Note:** For the Work and personal - user privacy activation types, only BlackBerry devices powered by Android 8.x and later support this command.	MDM controls Work and personal - full control (Samsung KNOX) Work space only (Android Enterprise) Work and personal - full control (Android Enterprise) Work and personal - user privacy (Android Enterprise)
Reset work space password	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.	Work and personal - full control (Samsung KNOX) Work and personal - user privacy - (Samsung KNOX) Work space only - (Samsung KNOX)
Specify work space password and lock	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.	Work and personal - user privacy (Android Enterprise) Work and personal - full control (Android Enterprise)
Disable/enable work space	This command disables or enables access to the work space apps on the device.	Work and personal - full control (Samsung KNOX) Work and personal - user privacy - (Samsung KNOX) Work space only - (Samsung KNOX)
Deactivate BlackBerry 2FA	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.	BlackBerry 2FA

Command	Description	Activation types
Wipe apps	This command wipes data from all Microsoft Intune-managed apps on the device. The apps are not removed from the device. For more information, see Wipe apps managed by Microsoft Intune	All (except BlackBerry 2FA)

Legal notice

©2019 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