BlackBerry UEM

Overview and What's New

12.12.1

Contents

What's new in BlackBerry UEM 12.12 MR1

- **App installation ranking for Google Play apps**: BlackBerry UEM now supports app installation ranking for Google Play apps on devices that are activated with Android Enterprise. The ranking of apps hosted in BlackBerry UEM and apps hosted in Google Play is applied separately.
- **Migration**: You can now migrate BlackBerry Dynamics users from one on-premises BlackBerry UEM instance to another on-premises BlackBerry UEM instance.

New IT policy rules

Device	Name	Description	Activation type
Android Global rule - Samsung Knox devices only	Force Bluetooth discoverable mode	Specify whether Bluetooth discoverable mode is enabled on the device. If this rule is selected the device is always available for incoming Bluetooth connection requests. If this rule is not selected and the user turns on Bluetooth , the device is not visible to other devices.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)

What's new in BlackBerry UEM 12.12

iOS

- **Apple DEP error message update**: If you have not yet accepted the updated terms and conditions for Apple Business Manager, you will receive an error message by email.
- **Synchronize Apple DEP accounts with Apple Business Manager manually**: You can manually synchronize Apple DEP accounts in BlackBerry UEM to ensure device connectivity.
- **Event notification update**: The Apple DEP connection failure status event notification now contains details for Communication Status, Operation mode, and Last synchronization time.
- **Specify activation profile for Apple DEP devices**: For each device registered in Apple DEP, you can now specify the activation profile that you want to assign to it. For example, if a user has multiple iOS devices that require different activation types, you can specify the activation profile for each device. When activating theiOS device, the activation profile that is assigned to the device takes precedence over the activation profile that is assigned to the user account.
- **Assign users directly to Apple DEP device serial numbers**: BlackBerry UEM now allows you to assign a user to an Apple DEP device serial number before the device is activated. When a user is assigned to the device serial number in the BlackBerry UEM management console, the user is not prompted for a username or password during device activation.
- **Update iOS to specific version number**: On the device tab, you can upgrade the software version on a supervised iOS device to a specific version number. You can use this feature to update the device OS to a version that your organization's IT department has certified.
- **Support for iOS 13 single sign-on extension**: Single sign-on extension for iOS 13 and iPadOS 13 allows users to authenticate once and then automatically log in to domains and web services within your organization's network. You can configure a single sign-on extension profile in BlackBerry UEM for devices running iOS (or iPadOS) 13.
- **Improved activation process**: The BlackBerry UEM Client for iOS has been updated to add some safeguards to minimize the instances where a user must restart the activation process from the beginning due to an interruption during device activation (for example, the user receives a call during activation). When the user returns to the UEM Client, the user can now resume activation from the most recent step.
- **New activation type for iOS and iPadOS 13.1 devices**: A new activation type "User privacy – User enrollment" is now available for unsupervised iOS devices running iOS or iPadOS 13.1 and later. The activation type helps maintain user privacy while keeping work data separated and protected. Administrators can manage work data (for example, wipe work data) without affecting personal data. To activate a device with this activation type, users can simply use the native camera app to scan the QR Code that they received in the activation email to manually download and install the MDM profile to the device. To activate their device, the user logs in to their managed Apple ID account. Administrators can also assign the BlackBerry UEM Client to allow users to easily activate other BlackBerry Dynamics apps, import certificates, use 2FA features, use CylancePROTECT Mobile for BlackBerry UEM, and check their compliance status.
- **Support for iOS 13 features**: BlackBerry UEM supports the new capabilities in iOS 13. New support includes three new IT policy rules, support for WPA-3 Personal and WPA-3 Enterprise Wi-Fi security, and new Email profile, VPN profile, and App Lock Mode profile settings.

Android

- **Factory reset protection profile**: You can specify multiple Google accounts to a Factory reset protection profile.
- **Improvements to Android Enterprise device activation user experience**: The number of steps required to activate Android Enterprise devices has been reduced. Users can now tap a check box when they enter their username to accept the license agreement. Additional notifications have been added to show app installation progress. Additional messages have been added to describe permissions required by the UEM Client.

- **Updated activation error messages**: When activation is not successful on an Android device, a new or updated error message displays that explains why the device did not activate properly. This allows the user and IT personnel to diagnose and fix the problem.
- **Use OEMConfig apps from Android device manufacturers to manage device features**: BlackBerry UEM supports using OEMConfig apps provided by device manufacturers, (for example, the Samsung Knox Service Plugin), to manage manufacturer-specific APIs on devices. The Samsung Knox Service Plugin allows you to manage new Samsung device features as soon as Samsung updates the device and app instead of waiting for new profile settings and IT policy rules in the next UEM update.
- **Review feedback from Android apps with app configurations**: BlackBerry UEM receives and displays error and information feedback from any Android apps that have an app configuration and have been developed to provide feedback.
- **Easily add work apps for Android Enterprise devices to Google Play**: Access the updated Google Play interface from BlackBerry UEM to more easily add private apps and web apps (shortcuts to web pages) to Google Play in the work profile on Android Enterprise devices. Note that this feature is now available if you are using BlackBerry UEM 12.9 MR1 or later.
- **Corporate owned single-use (COSU) device support for Android Enterprise**: BlackBerry UEM now supports corporate owned single-use for Android Enterprise version 9.0 and later. When configured for COSU, a device is locked to a specific set of applications to perform a function.
- **Request bug report**: You can now send a command to an Android Enterprise device from BlackBerry UEM to request the client logs. Request bug report is available for the following activation types:
  - Work space only (Android Enterprise fully managed device)
  - Work and personal – full control (Android Enterprise fully managed device with work profile)
- **Control runtime permissions for Android apps**: When you add an Android app in BlackBerry UEM, you can choose to set runtime app permissions. You can choose to grant permissions, deny permissions, or use an app permission policy for each permission listed for the app.
- **Send client download location with QR Code**: You can define the location for downloading the UEM Client for Work space only (Android Enterprise fully managed device) and Work and personal – full control (Android Enterprise fully managed device with work profile) activation types. The location is sent in the QR Code.
- **Date range for OS updates**: For Android Enterprise Work space only and Work and personal – full control devices, you can now specify a date range when OS updates should not occur.
- **Message displays when work profile is deleted**: If you use the "Delete only work data" command for Android Enterprise Work and personal - user privacy devices, you can provide a reason that appears in the notification on the user's device to explain why the work profile was deleted.
- **Message displays when work profile is deleted due to a compliance violation**: If the work profile is deleted from an Android Enterprise Work and personal - user privacy device due to a compliance violation, the notification on the device now describes the compliance rule that was broken.
- **Force device restart**: You can now use the Restart device command to force Android Enterprise Work space only and Work and personal – full control devices to restart.
- **Improved secure tunnel connection for Android devices**: When an Android device enters Doze mode, the BlackBerry Secure Connect Plus connection is now more reliably maintained.
- **Default device SR profile and work app updates**: There is now a default device SR profile that is assigned to user accounts that don't already have a device SR profile assigned. The default profile is configured for Android devices only and has the "Enable update period for apps that are running in the foreground" option enabled which allows work apps from Google Play to be automatically updated during the time period. By default, apps are scheduled to start updates daily over Wi-Fi at 02:00 (local device time) and stop in 4 hours.
- **Limit Android Enterprise devices to a single app**: The app lock mode profile is now supported for devices that are running Android 9 or later and activated with the “Work space only (Android Enterprise fully managed device)” activation type. You can now use the profile to limit Android Enterprise devices to the apps that you specify and, optionally, limit the device to a single app. When you limit the device to a single app, the app can access the other apps that you specified in the profile when it is required, but users always return to the app that the device is limited to.

Samsung Knox

- **Support for Samsung Knox DualDAR**: Devices that support Samsung Knox DualDAR encryption can now have Knox Workspace data secured using two layers of encryption. When the user is not using the device, all data in the Knox Workspace is locked and can't be accessed by apps running in the background. In the Activation profile, you can specify whether to use the default DualDAR app or an internal app to encrypt the workspace. In the Device profile, you can specify the data lock timeout after which the user must authenticate with both device and workspace to access work data again, and specify apps that are allowed to access work data even when work data is locked.

  Samsung Knox DualDAR encryption is supported on devices that run Samsung Knox 3.3 or later for new activations using the Work and personal - full control (Android Enterprise fully managed device with work profile) premium activation type.
- **Improved support for Knox Platform for Enterprise devices**: Samsung Knox IT policies were added for devices that support Knox Platform for Enterprise. These policies are applied to the device, personal space, or work spaces on the device depending on the Android Enterprise activation type that you choose. Support has also been added for native Samsung VPN and email, the ability to restrict apps in the personal space, and the ability to remotely lock the work space. To use Knox Platform for Enterprise features, the Knox device must be running Android 8 or later and be activated with one of the Android Enterprise activation types and the premium option enabled.

Windows

- **BitLocker encryption policies for Windows10 devices**: Several IT policies that support the use of BitLocker Drive Encryption were added to UEM for Windows10 devices that require encryption. When configured, the devices prompt users to encrypt data using BitLocker on their OS drives, fixed data drives, and removable storage drives. You can configure the encryption strength, the additional authentication requirements and the PIN options for devices that have a Trusted Platform Module, and the recovery options that you want to allow (for example, if a user is locked out of their device).

Installation and Upgrade

- **Regionalization**: BlackBerry UEM version 12.12 introduces regionalization features that allow BlackBerry Dynamics traffic to use the BlackBerry Infrastructure instead of the BlackBerry Dynamics NOC. These features are on by default in new installations of BlackBerry UEM version 12.12. If you are upgrading to BlackBerry UEM version 12.12 and want to enable these features, contact BlackBerry Technical Support. The regionalization features require BlackBerry Dynamics apps released in February 2020 or later. For custom BlackBerry Dynamics apps, BlackBerry Dynamics SDK 7.0 or later is required.
- **Migration support**: BlackBerry UEM version 12.12 supports migrations from BlackBerry UEMversion 12.10 and later, and from Good Control version 5.0.
- **Upgrade support**: BlackBerry UEM version 12.12 supports upgrades from BlackBerry UEM version 12.10 and later.
- **BES5 support**: BES5 will no longer be integrated with BlackBerry UEM.

Software support

As of version 12.12, BlackBerry UEM no longer supports the following software:

- iOS version 11: (visit support.blackberry.com to read KB57538)
- Android OS version 6 (visit support.blackberry.com to read KB57539)
- BlackBerry 10 OS (see the BlackBerry Software Lifecycle Overview)
- Windows Server 2008

Management console

- **Compliance profile updates**: In a compliance profile, you can now set the Enforcement action for BlackBerry Dynamics apps to Monitor and log. For new compliance profiles, 'Monitor and log' is now the default setting. The default option for Prompt interval expired action is also 'Monitor and log'.
- **Improvements to device filtering**: You can now filter devices by model number. For example, you can now filter different Samsung Galaxy device models such as Samsung A5 SM-A520F and Samsung A5 SM-A510F. This allows administrators to apply policies, profiles, and group status to multiple devices of a specific model.
- **App configuration**: When you add a new version of an internal app to BlackBerry UEM, the app configuration is automatically copied from the older version of the internal app to the new version.
- **Event notification update**: The "Metadata updated" event notification has been improved to display the full name of the device hardware vendor.
- **Override BlackBerry Dynamics connectivity profile on a per-app basis**: You can now specify a BlackBerry Dynamics connectivity profile to associate with each BlackBerry Dynamics app in BlackBerry UEM. When a profile is assigned to an app, that profile takes precedence over the profile assigned to the user of that app.
- **App shortcut filter**: A new filter on the UEM management console Apps page lets you search for app shortcuts.
- **Dedicated device groups**: BlackBerry UEM has a new Dedicated devices menu item. You can view, add, edit, and delete shared device groups and public device groups under the Dedicated devices menu. Public device groups are used to manage single-use devices that are not assigned to specific users. Shared device groups are used to manage devices that can be checked out by multiple users. Previously, shared device groups were located under the Users menu item.
- **Microsoft Azure single tenant application registration**: When you add or edit a Microsoft Azure Active Directory Connect connection, you can choose to enable single tenant application registration.
- **Restrict enrollment using device IDs**: On the Activation defaults page, you can import and export a list of unique device identifiers to restrict which devices can enroll with BlackBerry UEM. You can specify whether BlackBerry UEM can limit activation by device ID in the following activation types:

  Android

  - Work space only (Android Enterprise fully managed device)
  - Work and personal – full control (Android Enterprise fully managed device)

  iOS

  - MDM controls

BlackBerry Dynamics

- **Configure BlackBerry Dynamics proxy settings with a PAC file**: You can now use a PAC file to configure HTTP proxy settings for app traffic connections to the BlackBerry Dynamics NOC. PAC files are supported only for apps that use BlackBerry Dynamics SDK version 7.0 and later.
- **TLS v1.2**: BlackBerry Dynamics apps now allow only TLS v1.2 for secure communications by default. To allow TLSv1 and v1.1, you must manually configure them.

New IT policy rules

- **Access Point Name profile**: You can use Access Point Name profiles to send APNs for carriers to your user's Android devices. If you want to force a device to use an APN sent to it by an Access Point Name profile, you can use the "Force device to use Access Point Name profile settings" IT policy rule in the Android Global IT policy rules.
- **Hide certificate**: For certificates pushed to Android Enterprise devices with Android 9.0 and later, SCEP, shared certificate, and user credential profiles now allow you to hide the certificate from users to prevent them for using it for unintended purposes.

Device Type	Name	Description	Activation types
iOS	Allow Files app to use USB (supervised only)	Specify whether the Files app can access files using a USB connection.	MDM controls
iOS	Allow Files app to connect to network drives (supervised only)	Specify whether the Files app can access files stored on a network drive.	MDM controls
iOS	Force Wi-Fi to be enabled (supervised only)	Specify whether Wi-Fi is always enabled on the device. If this rule is selected, users can't turn Wi-Fi off using the Device Settings or Control Center and Airplane Mode doesn't disable Wi-Fi.	MDM controls
iOS	Allow Files app to connect to network drives (supervised only)	Specify whether the Files app can access files stored on a network drive.	MDM controls
macOS	Enable Bluetooth	Specify whether Bluetooth is enabled or disabled when the policy is sent to the device. Regardless of the setting for rule, users can change the Bluetooth setting on their device at any time.	MDM controls
Android Global (all Android devices)	Secondary authentication timeout	Specify the maximum amount of time, in hours, that the user can use secondary authentication methods, such as a fingerprint, before the user must unlock the device with a strong authentication method such as a password. The maximum is 72 hours. If set to 0, a timeout value is not sent to the device. This rule takes effect only if the "Password requirements" rule is set	Work space only, Work space only (Premium), Work and personal - user privacy, Work and personal - user privacy (Premium), Work and personal - full control, Work and personal - full control (Premium)

		to something other than "Unspecified."	
Android Global (all Android devices)	Allow installation of non-Google Play apps	Specify whether users can install apps from sources other than Google Play(unknown sources) globally on the device for all users. If you disallow installation of non-Google Playapps using this rule, the settings for the same rule in personal and work profiles are ignored. If this rule is selected, you can disallow installation of non-Google Playapps in just the work profile or just the personal profile.	Work space only, Work space only (Premium), Work and personal - user privacy, Work and personal - user privacy (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Require internal storage encryption	Specify if a user is prompted to encrypt the device memory and the internal SD card on a device. If this rule is selected, remote administration commands such as changing a password or wiping the device cannot be applied unless the device is already running and the user can log in (or is logged in). This rule requires the value of the "Password requirements" rule to be at least "Alphanumeric". The device memory and internal SD card needs to be encrypted by the user prior to an activation in order for an activation to complete.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Enable USB debugging	Specify if debugging over a USB connection is available. If this rule is not selected, debugging using Dalvik Debug Monitor Service (DDMS)	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)

		is also blocked. This rule is available only if the Allow developer mode rule is selected.	
Android Global (Samsung Knox devices only)	Allow outgoing SMS	Specify if a device can send SMS messages.	Work space only, Work space only (Premium),Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Allow incoming SMS	Specify if a device can receive SMS messages.	Work space only, Work space only (Premium),Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Allow users to modify the mock location	Specify if a user can enable or disable mocking a device's GPS location. If this rule is selected, the device can change its actual longitude and latitude readings, and GPS apps show the false coordinates instead of the actual coordinates. This rule is available only if the Allow developer mode rule is selected.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Maximum numeric sequence length	Specify the maximum length of the numeric sequence that is allowed in the device password. Only applies when device password quality is Numeric, Alphanumeric or Complex.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Minimum number of changed characters for new device passwords	Specify the minimum number of changed characters that a new password must include compared to the previous password. Knox calculates the difference between the two passwords using the Levenshtein	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)

		algorithm. Characters can be numeric, alphabetic, or symbolic. According to the Levenshtein algorithm, strings like "test" and "best" differ from each other by one unit. "Test" and "toad" differ from each other by three units. "Test" and "est" differ from each other by one unit. If set to 0, no restrictions are applied.	
Android Global (Samsung Knox devices only)	Allow device password visibility	Specify whether the Device password is visible when a user is typing it. If this rule is not selected, users and apps cannot change the visibility setting.	Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Require lock screen message	Specify whether you set a message to display when the device is locked. If this rule is not selected, the user can choose a message to display on the lock screen.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Lock screen message	Specify the text to display on the device when the device is locked.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Maximum character sequence length	Specify the maximum length of the character sequence that is allowed in the device password. Only applies when device password quality is Alphabetic, Alphanumeric or Complex.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only	Allow phone	Specify if a user can use the phone. If this rule is not selected, the device can only make	Work space only, Work space only (Premium), Work and personal - full control, Work and

		emergency calls. All other calls are blocked.	personal - full control (Premium)
Android Global (Samsung Knox devices only	Allow date and time changes	Specify if a user can manually change the date and time setting on a device.	Work space only (Premium), Work space only, Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only	Force automatic time sync	Specify if the device must obtain the date and time automatically using NITZ. If this rule is not selected, the user can choose whether the device automatically syncs the date and time.	Work space only (Premium), Work space only, Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only	Allow Native Samsung VPN	Specify if a user can use the native VPN functionality. If this rule is not selected, the user cannot open a VPN session or access the VPN settings in the Settings app.	Work space only (Premium), Work space only, Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only	Allow WAP push while roaming	Specify if a device can receive WAP push messages when roaming. If this rule is not selected, the device cannot receive MMS messages when roaming and the user cannot change this setting on the device. This rule applies only when the device is roaming.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only	Allow automatic sync while roaming	Specify whether a device can synchronize data automatically while roaming. If this rule is not selected, a roaming device can synchronize data only when a user accesses an account and the user cannot change this setting on the device. This setting	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)

		applies only when the device is roaming.	
Android Global (Samsung Knox devices only	Allow voice calls while roaming	Specify if a device can make or receive voice calls while roaming.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Allow SD card	Specify if a device can access an SD card. If this rule is not selected, read and write access to the SD card is blocked.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Allow data on mobile network	Specify if a device can use a mobile network connection. If this rule is not selected, the device cannot use the SIM data connection.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Allow users to add new Wi-Fi networks	Specify whether users can add new Wi-Fi profiles to the device. If this rule is not selected, users can only use the work Wi-Fi profiles that you configure.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only)	Allow Android Beam	Specify whether users can use Android Beam or S Beam to send contact information, web bookmarks, and other data to a nearby device. Specify whether users can use AndroidBeam or S Beam to send contact information, web bookmarks, and other data to a nearby device.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Global (Samsung Knox devices only	Allow Media Transfer Protocol (MTP)	Specify if a device can use MTP. Because Androidsupports USB file transfer through MTP only, you can use this rule to block any kind	Work space only, Work space only (Premium), Work and personal - full control, Work and

		of file transfer through USB. Picture Transfer Protocol (PTP) is a subset of MTP and is also affected by this rule.	personal - full control (Premium)
Android Global (Samsung Knox devices only)	Allow USB host storage	Specify if a device can use USB host storage using USB OTG. If this rule is selected, a user can connect any pen drive (portable USB storage), external HD, or SD card reader, and it is mounted as a storage drive on the device. If this rule is not selected, a user cannot mount any external storage device.	Work space only, Work space only (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Work profile (all Android devices)	Secondary authentication timeout	Specify the maximum amount of time, in hours, that the user can use secondary authentication methods, such as a fingerprint, before the user must unlock the device with a strong authentication method such as a password. The maximum is 72 hours. If set to 0, a timeout value is not sent to the device. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified."	Work and personal - user privacy, Work and personal - user privacy (Premium), Work and personal - full control, Work and personal - full control (Premium)
Android Personal profile (Samsung Knox devices only)	Allow audio recording	Specify whether a device can record audio. If this rule is not selected, the user can still make calls and use audio streaming using the device microphone. This rule applies to phone calls, voice recognition, and VoIP. If an app declares a use type and does something else, then this rule cannot block the app. If you	Work and personal - full control (Premium)

		deselect this rule, any ongoing audio recording is interrupted. Video recording is still allowed if no audio recording is attempted. This rule applies to the Personal space only.	
Android Personal profile (Samsung Knox devices only)	Allow video recording	Specify whether a device can record video. If this rule is not selected, the camera is still available so that the user can take pictures and the user can use video streaming. When this rule is not selected, any ongoing video recording is interrupted.	Work and personal - full control (Premium)
Android Personal profile (Samsung Knox devices only)	Allow Google auto-sync	Specify if Google accounts and apps can sync automatically. This rule does not block Google Play from updating installed apps. Users can still manually sync from some apps, including Gmail.	Work and personal - full control (Premium)
Android Personal profile (Samsung Knox devices only)	Allow sending crash reports to Google	Specify if the user can send crash reports to Google.	Work and personal - full control (Premium)
Android Personal profile (Samsung Knox devices only)	Allow S Voice	Specify whether a device can use the S Voice app.	Work and personal - full control, Work and personal - full control (Premium)
Android Personal profile (Samsung Knox devices only)	Enforce two-factor authentication	Specify whether a user must use two-factor authentication to access the device. For example, you can use this rule if you want the user to authenticate using a fingerprint and a password.	Work and personal - full control (Premium)

Android Personal profile (Samsung Knox devices only)	Allow other device administration apps	Specify if a device can be managed by other apps, such as MDM apps, in addition to the BlackBerry UEM Client. If this rule is not selected and other device administration apps are activated before the policy is sent to the device, the policy cannot be applied.	Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow work files in the personal profile	Specify whether a user can move files from the work profile to the personal profile on a device.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow personal files in the work profile	Specify whether a user can move files from the personal profile to the work profile on a device.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Enable work and personal data synchronization	Specify if apps can synchronize data between the work profile and the personal profile.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow personal contacts in the work profile	Specify whether the contacts app can import personal contact data into the work profile.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow work contacts in the personal profile	Specify whether the contacts app can export work contact data from the work profile into the personal profile.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow personal calendar data in the work profile	Specify whether the calendar app can import personal calendar data into the work profile.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow work calendar data in the personal profile	Specify whether the calendar app can export work calendar from the work profile into the personal profile.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)

Android Work profile (Samsung Knox devices only)	Allow user modification of "Show detailed notifications" setting	Specify whether a user can change the "Show detailed notifications" setting on a device. This setting determines whether the device displays reduced information about work notifications in the personal profile.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Apps allowed to access external storage	Specify the package IDs of apps in the work profile that are allowed to read and write data to an SD card.	Work space only (Premium), Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow other device administration apps	Specify if a device can be managed by other apps, such as MDM apps, in addition to the BlackBerry UEM Client. If this rule is not selected and other device administration apps are activated before the policy is sent to the device, the policy cannot be applied.	Work and personal - user privacy (Premium), Work space only, Work space only (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow sending crash reports to Google	Specify if the user can send crash reports to Google.	Work and personal - user privacy (Premium), Work space only, Work space only (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Allow camera	Specify whether a user can use the camera in the work profile.	Work and personal - user privacy (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only	Allow S Voice	Specify whether a device can use the S Voice app.	Work space only (Premium), Work space only, Work and personal - full control, Work and personal - full control (Premium)

Android Work profile (Samsung Knox devices only)	Enforce two-factor authentication	Specify whether a user must use two-factor authentication to access the work profile. For example, you can use this rule if you want the user to authenticate using a fingerprint and a password.	Work and personal - user privacy (Premium), Work space only (Premium), Work and personal - full control (Premium)
Android Work profile (Samsung Knox devices only)	Maximum character sequence length	Specify the maximum length of the character sequence that is allowed in the work profile password. Only applies when work profile password quality is Alphabetic, Alphanumeric or Complex.	Work and personal - full control (Premium),Work and personal - user privacy (Premium)
Android Work profile (Samsung Knox devices only)	Maximum numeric sequence length	Specify the maximum length of the numeric sequence that is allowed in the work profile password. Only applies when work profile password quality is Numeric, Alphanumeric or Complex.	Work and personal - full control (Premium),Work and personal - user privacy (Premium)
Android Work profile (Samsung Knox devices only	Minimum number of changed characters for new work profile passwords	Specify the minimum number of changed characters that a new password must include compared to the previous password.	Work and personal - full control (Premium),Work and personal - user privacy (Premium)
Android Personal profile (all Android devices)	Allowed system apps	Specify the package IDs for the system apps that are installed in the personal space. If you remove apps from this list, the apps are deleted from the personal space on users' devices.	Work and personal - full control, Work and personal - full control (Premium)
Android Personal profile (Samsung Knox devices only)	Allow other device administration apps	Specify if a device can be managed by other apps, such as MDM apps, in addition to the BlackBerry UEM Client. If this rule is	Work and personal - full control (Premium)

		not selected and other device administration apps are activated before the policy is sent to the device, the policy cannot be applied.	
Windows	BitLocker encryption method for mobile	Specify the BitLocker Drive Encryption method and cipher strength for mobile devices. This rule does not apply to Windows 10 computers and tablets.	MDM controls
Windows	BitLocker encryption method for desktop	Specify the BitLocker Drive Encryption method and cipher strength for tablets and computers. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow storage card encryption prompts on the device	Specify whether the device prompts the user to encrypt the storage card. If this rule is not selected, encryption is not disabled. This rule does not apply to Windows 10 computers and tablets.	MDM controls
Windows	Allow BitLocker Device Encryption to enable encryption on the device	Specify whether BitLocker Device Encryption can enable encryption on the device. If this rule is not selected, encryption is not disabled but the user is not prompted to enable it.	MDM controls
Windows	Set default encryption methods for each drive type	Specify whether the default algorithm and cipher strength used by BitLocker Drive Encryption can be configured separately for different drive types. This rule does not apply to Windows 10 smartphones.	MDM controls

Windows	Encryption method for operating system drives	Specify the encryption method for operating system drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Encryption method for fixed data drives	Specify the encryption method for fixed data drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Encryption method for removable data drives	Specify the encryption method for removable data drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require additional authentication at startup	Specify whether BitLocker requires additional authentication each time the device starts. This setting is applied when BitLocker is turned on. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow BitLocker without a compatible TPM	Specify whether BitLocker can be started without a TPM chip. If this rule is selected, BitLocker can be started with a password or a startup key on a USB flash drive. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require TPM startup key	Specify whether a TPM startup key is optional, required, or disallowed. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require TPM startup PIN	Specify whether a TPM startup PIN is optional,	MDM controls

		required, or disallowed. This rule does not apply to Windows 10 smartphones.	
Windows	Require TPM startup key and PIN	Specify whether both a TPM startup key and PIN are optional, required, or disallowed. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require TPM startup	Specify whether TPM startup is optional, required, or disallowed. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require minimum PIN length for startup	Specify whether BitLocker has a minimum startup PIN length. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Minimum PIN length	Specify the minimum number of digits for the startup PIN. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Pre-boot recovery message and URL	Specify whether you can customize the BitLocker pre-boot recovery message and URL that are displayed on the pre-boot key recovery screen when the OS drive is locked. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Pre-boot recovery screen	Specify whether the BitLocker pre-boot recover screen is empty, displays a default message and URL, displays a custom message, or displays a custom	MDM controls

		URL. This rule does not apply to Windows 10 smartphones.	
Windows	Custom recovery message	If you selected "Custom recovery message" in the "Pre-boot recovery screen" rule, specify the custom message. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Custom recovery URL	If you selected "Custom recovery URL" in the "Pre-boot recovery screen" rule, specify the custom URL. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	BitLocker OS drive recovery options	Specify whether you can customize how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This setting is applied when you turn on BitLocker. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow certificate-based data recovery agent for OS drives	Specify whether a data recovery agent can be used with BitLocker-protected operating system drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow recovery password generation for OS drives	Specify whether the user can create and store a BitLocker recovery password for OS drives. This rule does not apply to Windows 10 smartphones.	MDM controls

Windows	Allow recovery key generation for OS drives	Specify whether the user can create and store a BitLocker recovery key for OS drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Exclude recovery options from the BitLocker setup wizard for OS drives	Specify whether recovery options are hidden from the user when they turn on BitLocker on an OS drive.	MDM controls
Windows	Allow saving BitLocker recovery information for OS drives to Active Directory Domain Services	Specify whether BitLocker recovery information for OS drives can be saved to Active Directory Domain Services. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Stored BitLocker recovery information for OS drives	Specify whether Active Directory Domain Services stores only recovery passwords, or both recovery passwords and key packages for OS drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require Active Directory backup for recovery information for OS drives	Specify whether BitLocker recovery information saved to Active Directory Domain Services for OS drives must be backed up. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	BitLocker fixed drive recovery options	Specify whether you can customize how BitLocker-protected fixed drives are recovered in the absence of the required startup key information. This setting is applied when you turn on BitLocker.	MDM controls

		This rule does not apply to Windows 10 smartphones.	
Windows	Allow certificate-based data recovery agent for fixed drives	Specify whether a data recovery agent can be used with BitLocker-protected fixed drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow recovery password generation for fixed drives	Specify whether the user can create and store a BitLocker recovery password for fixed drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow recovery key generation for fixed drives	Specify whether the user can create and store a BitLocker recovery key for fixed drives. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Exclude recovery options from the BitLocker setup wizard for fixed drives	Specify whether recovery options are hidden from the user when they turn on BitLocker on a fixed drive. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow saving BitLocker recovery information for fixed drives to Active Directory Domain Services	Allow BitLocker recovery information for fixed drives to be saved to Active Directory Domain Services. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Stored BitLocker recovery information for fixed drives	Specify whether Active Directory Domain Services stores only recovery passwords, or both recovery passwords and key packages for fixed drives. This rule does	MDM controls

		not apply to Windows 10 smartphones.	
Windows	Require Active Directory backup for recovery information for fixed drives	Specify whether BitLocker recovery information saved to Active Directory Domain Services for fixed drives must be backed up. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require BitLocker protection for fixed data drives	Specify whether BitLocker protection is required to allow write access to fixed data drives. If this rule is selected, all fixed data drives that are not BitLocker-protected will be mounted as read-only. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Require BitLocker protection for removable data drives	Specify whether BitLocker protection is required to allow write access to removeable data drives. If this rule is selected, all removeable data drives that are not BitLocker-protected will be mounted as read-only. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Allow write access to devices configured in another organization	Specify whether removable drives that don't match the device's identification fields can have write access. If this rule is selected, only drives with identification fields matching the computer's identification fields will be given write access. This rule does not apply to Windows 10 smartphones.	MDM controls

Windows	Allow recovery key location prompt	Specify whether the user is prompted to choose where to back up the OS drive's recovery key. When this rule is not selected, the OS drive's recovery key backs up to the user's Azure Active Directory account. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Enable encryption for standard users	Specify whether encryption is enabled on all fixed drives, even if a current logged in user is a standard user. This setting is only supported in Azure Active DirectoryWindows 10 smartphones.	MDM controls

What is BlackBerry UEM?

BlackBerry UEM is a multiplatform EMM solution from BlackBerry that provides comprehensive device, app, and content management with integrated security and connectivity, and helps you manage iOS, macOS, Android, Windows 10, and BlackBerry 10 devices for your organization.

You can install BlackBerry UEM in an on-premises environment for the utmost control over your servers, data, and devices, or you can use BlackBerry UEM Cloud, which offers an easy-to-use, low-cost, and secure solution. BlackBerry hosts BlackBerry UEM Cloud over the Internet. You only need a supported web browser to access the service.

Both BlackBerry UEM on-premises and BlackBerry UEM Cloud offer trusted end-to-end security and provide the control that organizations need to manage all endpoints and ownership models.

Benefits of BlackBerry UEM include:

Feature	Benefit
Low total cost of ownership	BlackBerry UEM on-premises reduces complexity, optimizes pooled resources, ensures maximum uptime and helps you achieve the lowest total cost of ownership for an on-premises solution. BlackBerry UEM Cloud reduces the cost of ownership by removing the need to install, manage, and update services.
Single web-based interface	Manage iOS, macOS, Android, Windows 10, and BlackBerry 10 devices plus additional BlackBerry Secure UEM & Productivity Suite services all from a single management console.
Flexible ownership models	Use a set of customizable policies and profiles to manage BYOD, COPE, and COBO devices, and protect business information.
User and device reporting	Manage fleets of devices using comprehensive reporting and dashboards, dynamic filters, and search capabilities.
Simple user setup and enrollment	Allow users to activate their own devices with BlackBerry UEM Self-Service.
Industry-leading mobile security	Leverage the BlackBerry Infrastructure to ensure data security across all devices.
High availability	Configure high availability on-premises to minimize service interruptions for device users or rely on BlackBerry to maintain BlackBerry UEM Cloud and maximize uptime for you.
Additional services available	Enable services such as BlackBerry Workspaces, BlackBerry Enterprise Identity, BlackBerry 2FA, BBM Enterprise, and BlackBerry UEM Notifications (BlackBerry UEM on-premises only) that allow you to add value to your BlackBerry UEM deployment.

For more information about BlackBerry UEM, see the Administration content.

BlackBerry enterprise services

Beyond the security and productivity features that BlackBerry UEM provides, BlackBerry offers more services that can add value to your BlackBerry UEM to help meet your organization's unique needs. You can add the following services and manage them through the BlackBerry UEM management console:

Service type	Service name and description
Enterprise services	• BlackBerry Workspaces allows users to securely access, synchronize, edit, and share files and folders from Windows and Mac OS tablets and computers or Android, iOS, and BlackBerry 10 devices. BlackBerry Workspaces protects files by applying DRM controls to limit access, even after they are shared with someone outside of your organization. • BlackBerry Enterprise Identity gives users single sign-on access to service providers, such as BlackBerry Workspaces, Box, Workday, WebEx, Salesforce, and more. You can also add support for custom SaaS services. • BlackBerry 2FA protects access to your organization's critical resources using two-factor authentication. BlackBerry 2FA uses a password that users enter and a secure prompt on their Android, iOS, or BlackBerry 10 devices each time they attempt to access resources.

BlackBerry Dynamics platform	• The BlackBerry Enterprise Mobility Server (BEMS) on-premises and BEMS-Cloud provides additional services for BlackBerry Dynamics apps.
	  • BEMS on-premises integrates the BlackBerry Mail, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs services. When these services are integrated, users can communicate with each other using secure email messages and instant messaging, view the real-time presence of users in BlackBerry Dynamics apps, and access, synchronize, and share work file server, Microsoft SharePoint, Microsoft SharePoint Online, Microsoft OneDrive for Business, and Box documents without putting work data at risk.
	  • BEMS-Cloud integrates the BlackBerry Mail and BlackBerry Docs services. When these services are integrated, users can communicate with each other using secure email messages and access, synchronize, and share Microsoft SharePoint, Microsoft SharePoint Online, Microsoft OneDrive for Business, and Box documents without putting work data at risk.
	• The BlackBerry Dynamics SDK allows developers to create secure apps for Android and iOS devices and Mac OS and Windows computers.

Service type	Service name and description
BlackBerry Dynamics productivity apps	• BlackBerry Work provides everything users need to securely mobilize their work, including email, calendar, and contacts (full synchronization with Microsoft Exchange). The app also provides advanced document collaboration. BlackBerry Work separates work data from personal data and allows seamless integration with other work apps without requiring MDM profiles on the device. • BlackBerry Access enables users to securely access their organization's intranet with their device. • BlackBerry Connect enhances communication and collaboration with secure instant messaging, corporate directory lookup, and user presence, all from an easy-to-use interface on the user's device. • BlackBerry Tasks allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their Android and iOS devices. • BlackBerry Notes allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their device.

These services can be purchased as part of a Suite license. For more information about the different Suites and how to obtain them, see the Licensing content.

BlackBerry Secure UEM & Productivity Suites

BlackBerry Secure UEM & Productivity Suites include BlackBerry UEM, BlackBerry Dynamics, and additional services under one license to offer a comprehensive unified endpoint management solution that provides mobile collaboration and a trusted end-to-end approach to security.

Suite	Features
BlackBerry Secure UEM & Productivity Suites – Choice Suite	• Cross-platform support for iOS, macOS, Android (including Samsung Knox), Windows 10, and BlackBerry 10 devices • BlackBerry UEM with support for Work and personal - Corporate activations for BlackBerry 10 devices, MDM controls for most device types, User privacy activations for iOS and Android devices, and Work and personal and Work space only activations for Android devices • BlackBerry Dynamics with support for MDM, MAM, BlackBerry Access, and BlackBerry Work • Secure instant messaging using BlackBerry Connect • Cloud and on-premises deployment options • Data gathering and usage metrics from BlackBerry Dynamics apps on your users' devices using BlackBerry Analytics

Suite	Features
BlackBerry Secure UEM & Productivity Suites – Freedom Suite	• All BlackBerry Secure UEM & Productivity Suites – Choice Suite features • Advanced BlackBerry UEM security and connectivity features for managing iOS, Android (including Samsung Knox Workspace and Knox Platform for Enterprise), and BlackBerry 10 devices • Secure access to work content using BlackBerry Secure Connect Plus and BlackBerry Docs • Unlimited deployment of BlackBerry Dynamics secured apps from third-party software vendors • Secure access to view, edit, and save documents using Intune managed Microsoft apps, such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel, in BlackBerry Dynamics apps on iOSand Android devices using BlackBerry Enterprise BRIDGE • Complete cloud service federation and single sign-on solution using BlackBerry Enterprise Identity • Unlimited deployment of customer-developed BlackBerry Dynamics secured apps • Custom shared services app integration • Full two-factor authentication enabled through users' devices with BlackBerry 2FA • Enterprise file synchronization, sharing, and access control with BlackBerry Workspaces
BlackBerry Secure UEM & Productivity Suites – Limitless Suite	• All BlackBerry Secure UEM & Productivity Suites – Freedom Suite features • Send messages to users via SMS, phone, and email directly from the BlackBerry UEM management console with UEM Notifications (BlackBerry UEM on-premises only) • Enterprise file synchronization, sharing, access control, document rights management across mobile devices, and SDK support with BlackBerry Workspaces

Benefits of BlackBerry Workspaces

BlackBerry Workspaces is an enterprise file management platform that allows users to securely access, synchronize, edit, and share files and folders across multiple devices. BlackBerry Workspaces limits the risk for data loss or theft by embedding digital rights management security into every file, so your content remains secure and within your control, even after it is downloaded and shared with others. With a secure file store and the ability to transfer data while maintaining control, both employees and IT can be confident in data sharing and document security.

Users can access BlackBerry Workspaces from a Web browser and from apps on Windows and macOS computers and on iOS, Android, and BlackBerry 10 devices. Content is synchronized across all of a user's devices when they are online, allowing users to manage, view, create, edit, and annotate files from any device. You can use the Workspaces plug-in for BlackBerry UEM to integrate Workspaces management into the BlackBerry UEM management console

If your organization also implements BlackBerry Enterprise Identity, you can use Enterprise Identity to manage user entitlement to Workspaces. For more information about Enterprise Identity see the BlackBerry Enterprise Identity content.

BlackBerry Workspaces can be purchased separately or licensed with BlackBerry Secure UEM & Productivity Suites – Freedom Suite. Additional features are included with BlackBerry Secure UEM & Productivity Suites – Limitless Suite.

For more information, see the BlackBerry Workspaces content.

Benefits of BlackBerry Enterprise Identity

BlackBerry Enterprise Identity makes it easy for users to access cloud applications from any device, including iOS, Android, and BlackBerry 10, as well as traditional computing platforms. This capability is tightly integrated with BlackBerry UEM, unifying industry-leading EMM with the entitlement and control of all your cloud services.

BlackBerry Enterprise Identity provides single sign-on (SSO) to cloud services such as Microsoft Office 365, G Suite, BlackBerry Workspaces, and many others. With single sign-on, users don't have to complete multiple log ins or remember multiple passwords. Administrators can also add custom services to Enterprise Identity to give users access to internal applications.

Administrators use the BlackBerry UEM management console to add services, manage users, and to add and manage additional administrators. The integration with BlackBerry UEM makes it easy to manage users and entitle them to access cloud applications and services from their devices. Using BlackBerry UEM, cloud services and mobile app binaries can be bundled together and then simply assigned to a user or group of users.

Enterprise Identity can be purchased separately or licensed with these BlackBerry Secure UEM & Productivity Suites

- Choice Suite
- Freedom Suite
- Limitless Suite

For more information about Enterprise Identity, see the BlackBerry Enterprise Identity content.

Benefits of BlackBerry 2FA

BlackBerry 2FA provides users with two-factor authentication to access your organization's resources. It allows you to use your users iOS, Android, and BlackBerry 10 devices as the second factor of authentication when users connect to your organization's resources. BlackBerry 2FA provides a simple user experience that prompts users for confirmation on their device when they attempt to access one of your resources.

For users who don't have a mobile device or have a mobile device that doesn't have sufficient connectivity to support the real-time BlackBerry 2FA, you can issue standards-based one-time password (OTP) tokens. The first authentication factor is the user's directory password, and the second authentication factor is a dynamic code that appears on the token's screen.

You manage BlackBerry 2FA from the BlackBerry UEM or BlackBerry UEM Cloud management console. BlackBerry 2FA is also integrated with BlackBerry Enterprise Identity. You can use BlackBerry 2FA to provide a second factor of authentication for the resources that you manage access to with Enterprise Identity.

BlackBerry 2FA can be purchased separately or licensed with these BlackBerry Secure UEM & Productivity Suites

- Freedom Suite
- Limitless Suite

For more information about BlackBerry 2FA, see the BlackBerry 2FA content.

Benefits of BlackBerry UEM Notifications

BlackBerry UEM Notifications takes advantage of the BlackBerry AtHoc Networked Crisis Communication system to allow administrators can send critical messages and notifications to users and groups from the UEM management console.

Because UEM Notifications allows administrators to manage devices and notifications within the UEM management console, they don't need to manage and reconcile user contact information across multiple systems or deal with access issues in external systems. UEM Notifications leverages contact information using Microsoft Active Directory synchronization. UEM Notifications also offers flexible delivery options, including Text-To-Speech voice calls, SMS, and email so that users get alerts using their preferred channel, which increases the likelihood of action and compliance.

Administrators can track and manage notifications sent, including detailed message status by delivery method. UEM Notifications uses FedRAMP-authorized delivery services and provides a comprehensive report of all sent messages and their statuses.

BlackBerry UEM Notifications can be purchased separately with BlackBerry UEM or licensed with BlackBerry Secure UEM & Productivity Suites – Limitless Suite. It is available for use with BlackBerry UEM on-premises only.

For more information about UEM Notifications, see the UEM Notifications content.

Enterprise apps

BlackBerry offers several enterprise apps that administrators can push to devices or users can install to help them access work data and be more productive.

Component	Description
BlackBerry UEM Client	The BlackBerry UEM Client allows BlackBerry UEM to manage iOS and Android devices. Users require the BlackBerry UEM Client to activate iOS or Android devices for mobile device management with BlackBerry UEM. Users can download the latest version of the BlackBerry UEM Client from the App Store for iOS devices and from Google Play for Android devices. After users activate their devices, the BlackBerry UEM Client allows users to do the following: • Verify whether their devices are compliant with the organization's standards • View the profiles that have been assigned to their user accounts • View the IT policy rules that have been assigned to their user accounts • Access work apps • Create access keys for BlackBerry Dynamics apps • Preauthenticate with BlackBerry 2FA • Access a software OTP code • Retrieve and email device log files • Deactivate their devices For more information, see the BlackBerry UEM Client content.
BlackBerry Dynamics apps	BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect provide users with access to work data and productivity tools. For more information, see the documentation for each app.

Component	Description
BBM Enterprise	BBM Enterprise adds a layer of end-to-end encryption for BBM messages sent between BBM Enterprise users in your organization and other BBM users inside or outside of your organization. BBM Enterprise is available for iOS, Android, BlackBerry 10, Windows, and macOS devices. BBM Enterprise uses a FIPS 140-2 validated cryptographic library. Your organization owns the encryption keys and no one else, not even BlackBerry, can access them. For most devices, you can use BlackBerry UEM to assign BBM Enterprise to users. After you enable users to use BBM Enterprise, users can download the BBM Enterprise app from the App Store, the Google Play store, or BlackBerry World. For more information about BBM Enterprise, see the BBM Enterprise content.
BlackBerry Enterprise BRIDGE	BlackBerry Enterprise BRIDGE is a Microsoft Intune app that is enabled for BlackBerry Dynamics. It allows you to securely view, edit, and save documents using Intune-managed Microsoft apps, such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel in BlackBerry Dynamics on iOS and Android devices. For more information about BlackBerry Enterprise BRIDGE, see the BlackBerry Enterprise BRIDGE content.

BlackBerry Dynamics apps

BlackBerry Dynamics productivity apps provide users with access to work data and productivity tools. BlackBerry Dynamics apps developed by BlackBerry include the following:

App	Description
BlackBerry Work	The BlackBerry Work app provides secure access to work email and allows users to view and send attachments, create custom contact notifications, and manage their messages. For more information about BlackBerry Work, see the BlackBerry Work content.
BlackBerry Access	BlackBerry Access is a secure browser that allows users to access work intranets and web applications. BlackBerry Access also allows you to enable access to work resources or build and deploy rich HTML5 apps, while maintaining a high level of security and compliance. For more information about BlackBerry Access, see the BlackBerry Access content.
BlackBerry Connect	BlackBerry Connect allows communication and collaboration with secure instant messaging, company directory lookup, and user presence from an easy-to-use interface on the user's device. For more information about BlackBerry Connect, see the BlackBerry Connect content.
BlackBerry Tasks	BlackBerry Tasks allows users to create, edit, and manage tasks that are synchronized with Microsoft Exchange. For more information about BlackBerry Tasks, see the BlackBerry Tasks content.

App	Description
BlackBerry Notes	BlackBerry Notes allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their mobile device of choice. For more information about BlackBerry Notes, see the BlackBerry Notes content.

You can also use BlackBerry Dynamics apps developed by one of BlackBerry's many third-party application partners. For a full list of publicly available apps, visit the BlackBerry Marketplace for Enterprise Software.

You can also develop your own BlackBerry Dynamics apps using the BlackBerry Dynamics SDK. For more information, see the BlackBerry Dynamics SDK content.

Enterprise SDKs

BlackBerry offers several SDK options to help your organization customize and extend your BlackBerry solution.

Component	Description
BlackBerry UEM Integration SDK	The BlackBerry UEM Integration SDK allows developers to create plug-ins that extend the functionality of BlackBerry UEM. Using the UEM Integration SDK (which includes the UEM Integration plug-in for Eclipse) and the UEM Integration APIs, you can create and deploy BlackBerry UEM plug-ins that allow for the tight integration of new features or services with an existing BlackBerry UEM installation. For more information about the BlackBerry UEM Integration SDK, see the BlackBerry UEM Integration SDK content.
BlackBerry Dynamics SDK	The BlackBerry Dynamics SDK provides a powerful set of tools to ISV and enterprise developers, allowing them to focus on building their apps rather than learning how to secure, deploy, and manage those apps. The BlackBerry Dynamics SDK can be used to develop native, hybrid, and web apps for iOS, macOS, Android, and Windows devices, with services such as the following: • Security services (for example, secure communications and interapp data exchange APIs) • Mobile services (for example, presence, email, push, directory lookup) • Platform services (for example, single sign-on authentication, identity and access management, app-level controls for admins) For more information about the BlackBerry Dynamics SDK, see the BlackBerry Dynamics SDK content.
BlackBerry Analytics SDK	The BlackBerry Analytics SDK allows BlackBerry Dynamics app developers to enable custom BlackBerry Dynamics apps for Android and iOS to automatically record events and send them to BlackBerry Analytics. All you need to do is integrate the BlackBerry Analytics library into your app; the SDK does the work of sending the events for you. For more information about the BlackBerry Analytics SDK, see the BlackBerry Analytics content.

Component	Description
Spark Communications Services SDK	The BlackBerry Spark Communications Services SDK provides a framework to develop real-time, end-to-end secure messaging capabilities in your own product or service. The Spark Communications Services security model ensures that only the sender and intended recipient can see each message sent, and that messages aren't modified in transit between the sender and recipient. The Spark Communications Services SDK also provides the framework for other forms of collaboration and communication, such as push notifications, secure voice and video calls, and file sharing. You can even extend and create new types of real-time services and use cases by defining your own custom application protocols and data types. For more information about the Spark Communications Services, see the Spark Communications Services SDK content.
BlackBerry Web Services	The BlackBerry Web Services are a collection of SOAP and REST web services that you can use to create applications to manage your organization's BlackBerry UEM domain, user accounts, and all supported devices. You can use the BlackBerry Web Services to automate many tasks that administrators typically perform using the management console. For example, you can create an application that automates the process of creating user accounts, adds users to multiple groups, and manages users' devices. For more information about the BlackBerry Web Services, see the BlackBerry Web Services for BlackBerry UEM content.

For more information on obtaining and using all of the developer tools available from BlackBerry, visit the the BlackBerry Developers site.

Key BlackBerry UEM features

Feature	Description
Multiplatform device management	You can manage iOS, macOS, Android, Windows 10, and BlackBerry 10 devices.
Single, intuitive UI	You can view all devices in one place and access all management tasks in a single, web-based UI. You can share administrative duties with multiple administrators who can access the management console at the same time. You can toggle between default and advanced views to see options for displaying information and filtering the user list.
Trusted and secure experience	Device controls give you precise management of how devices connect to your network, what capabilities are enabled, and what apps are available. Whether the devices are owned by your organization or your users, you can protect your organization's information.
Separate work and personal needs	You can manage devices using Android Enterprise Samsung Knox, and BlackBerry Balance technologies that are designed to make sure that personal information and work information are kept separate and secure on devices. If the device is lost or the employee leaves the organization, you can delete only work-related information or all information from the device.
Secure IP connectivity	You can use BlackBerry Secure Connect Plus to provide a secure IP tunnel between work space apps on BlackBerry 10, iOS, Samsung Knox Workspace, and Android devices that have a work profile and your organization’s network. This tunnel gives users access to work resources behind the organization’s firewall while making sure the security of data using standard IPv4 protocols (TCP and UDP) and end-to-end encryption.
Simple user self-service	BlackBerry UEM Self-Service reduces support requests and lowers IT costs for your organization while giving users the option to manage their devices in a timely manner. Using BlackBerry UEM Self-Service, users can perform tasks like activating or switching devices, changing their device passwords remotely, deleting device data, or lock their lost or stolen devices, and address other critical support requirements.
Integration with services such as BlackBerry Workspaces, BlackBerry Enterprise Identity, and BlackBerry 2FA	You can integrate BlackBerry UEM with BlackBerry Workspaces, BlackBerry Enterprise Identity, and BlackBerry 2FA that allow you to add value to your organization's BlackBerry UEM instance.

Feature	Description
Powerful app management	BlackBerry UEM is a comprehensive app management platform for all devices. You can deploy apps from all major app stores, including App Store, Google Play, Windows Store, and BlackBerry World storefront.
Role-based administration	You can share administrative duties with multiple administrators who can access the administration consoles at the same time. You can use roles to define the actions that an administrator can perform and reduce security risks, distribute job responsibilities, and increase efficiency by limiting the options available to each administrator. You can use predefined roles or create your own custom roles.
Company directory integration	You can use local, built-in user authentication to access the management console and self-service console, or you can integrate with the Microsoft Active Directory or LDAP company directories that you use in your organization's environment (for example, IBM Domino Directory). BlackBerry UEM supports connections to multiple directories. You can have any combination of both Microsoft Active Directory and LDAP. You can also configure BlackBerry UEM to automatically synchronize the membership of a directory-linked group to its associated company directory groups when the scheduled synchronization occurs. When you configure the settings for directory-linked groups, you can select offboarding protection. Offboarding protection requires two consecutive synchronization cycles before device data or user accounts are deleted from BlackBerry UEM. This feature helps to prevent unexpected deletions that can occur because of latency in directory replication. To integrate BlackBerry UEM Cloud with your company directory you must install the BlackBerry Connectivity Node. You can install one or more instances of the BlackBerry Connectivity Node.
High availability	If you have BlackBerry UEM Cloud, instead of having to maintain your own highly available service for device management, with all the upfront and maintenance costs, BlackBerry maintains the service and maximizes uptime for you.

Feature	Description
Migration	You can migrate users, devices, groups, and other data from an on-premises BlackBerry UEM source database to a new on-premises or BlackBerry UEM Cloud instance. If you have configured BlackBerry UEM to manage Google Play accounts can migrate Android Enterprise devices from an on-premises BlackBerry UEM server to BlackBerry UEM Cloud or another on-premises BlackBerry UEM server. You can migrate BlackBerry Dynamics users from on-premises BlackBerry UEM (version 12.13 or later) to a BlackBerry UEM Cloud.
Cisco ISE integration	Cisco Identity Services Engine (ISE) is network administration software that gives an organization the ability to control whether devices can access the work network (for example, permitting or denying Wi-Fi or VPN connections). You can create a connection between Cisco ISE and BlackBerry UEM on-premises so that Cisco ISE can retrieve data about the devices that are activated on BlackBerry UEM. Cisco ISE checks device data to determine whether devices comply with your organization's access policies.
Regional deployment	You can set up regional connections for enterprise connectivity features by deploying one or more BlackBerry Connectivity Node instances in a dedicated region. This is known as a server group. Each BlackBerry Connectivity Node includes BlackBerry Secure Connect Plus, the BlackBerry Gatekeeping Service, the BlackBerry Secure Gateway, BlackBerry Proxy, and the BlackBerry Cloud Connector. You can associate enterprise connectivity and email profiles with a server group so that any users who are assigned those profiles use a specific regional connection to the BlackBerry Infrastructure when using BlackBerry Connectivity Node components. Deploying more than one BlackBerry Connectivity Node in a server group also allows for high availability and load balancing.
Wearable devices	You can activate and manage certain Android-based, head-worn wearable devices in BlackBerry UEM. For example, you can manage Vuzix M300 Smart Glasses. 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 bar-codes and use GPS navigation. Examples of BlackBerry UEM management capabilities that are supported include: Device activation using QR code, IT policies, Wi-Fi and VPN profiles, app management and location services.

Feature	Description
Microsoft Intune integration	For iOS and Android devices, if you want to protect data in Microsoft Office 365 apps using the MAM features of Microsoft Intune, you can use Intune to protect app data while using BlackBerry UEM to manage the devices. Intune provides security features that protect data within apps. For example, Intune can require that data within apps be encrypted and prevent copying and pasting, printing, and using the Save as command. You can connect UEM to Intune, allowing you to manage Intune app protection policies from within the UEM management console.

Key features for all device types

There are activities that you can perform with all of the device types that BlackBerry UEM supports. These include activation, management of devices, apps and licenses, controlling how devices connect to your organization's resources, and enforcing your organization's requirements. For more information about these features, see the following table.

Feature	Description
Activate devices	When you activate a device, you associate the device with your organization's environment so that users can access work data on their devices. You can activate a device with just an email address and activation password. You can allow users to activate devices themselves or you can activate devices for users and then distribute the devices. All device types can be activated over the wireless network.
Manage devices	You can view all devices in one place and access all management tasks in a single, web-based UI. You can manage multiple devices for each user account and view the device inventory for your organization. You can perform the following actions if the actions are supported by the device: • Lock the device, change the device or work space password, or delete information from the device • Connect the device securely to your organization's mail environment, using Microsoft Exchange ActiveSync for email and calendar support • Control how the device can connect to your organization's network, including Wi-Fi and VPN settings • Configure single sign-on for the device so that it authenticates automatically with domains and web services in your organization's network • Control the capabilities of the device, such as setting rules for password strength and disabling functions like the camera • Manage app availability on the device, including specifying app versions and whether the apps are required or optional • Search app stores directly for apps to assign to devices • Install certificates on the device and optionally configure SCEP to permit automatic certificate enrollment • Extend email security using S/MIME or PGP
Manage groups of users, apps, and devices	Groups simplify the management of users, apps, and devices. You can use groups to apply the same configuration settings to similar user accounts or similar devices. You can assign different groups of apps to different groups of users, and a user can be a member of several groups.
Control which devices can access Microsoft Exchange ActiveSync	You can use gatekeeping in BlackBerry UEM to ensure that only devices managed by BlackBerry UEM can access work email and other information on the device and meet your organization's security policy.

Feature	Description
Control how devices connect to your organization's resources	You can use an enterprise connectivity profile to control how apps on devices connect to your organization’s resources. When you enable enterprise connectivity, you avoid opening multiple ports in your organization's firewall to the Internet for device management and third-party applications such as the mail server, certification authority, and other web servers or content servers. Enterprise connectivity sends all traffic through the BlackBerry Infrastructure to BlackBerry UEM on port 3101.
Manage work apps	On all managed devices, work apps are apps that your organization makes available for its users. You can search the app stores directly for apps to assign to devices. You can specify whether apps are required on devices, and you can view whether a work app is installed on a device. Work apps can also be proprietary apps that were developed by your organization or by third-party developers for your organization's use.
Enforce your organization's requirements for devices	You can use a compliance profile to help enforce your organization's requirements for devices, such as not permitting access to work data for devices that are jailbroken, rooted, or have an integrity alert, or requiring that certain apps be installed on devices. You can send a notification to users to ask them to meet your organization's requirements, or you can limit users' access to your organization's resources and applications, delete work data, or delete all data on the device.
Send an email to users	You can send an email to multiple users directly from the management console. The users must have an email address associated with their account.
Create or import many user accounts with a .csv file	You can import a .csv file into BlackBerry UEM to create or import many user accounts at once. Depending on your requirements, you can also specify group membership and activation settings for the user accounts in the .csv file.
View reports of user and device information	The reporting dashboard displays an overview of your BlackBerry UEM environment. For example, you can view the number of devices in your organization sorted by service provider. You can view details about users and devices, export the information to a .csv file, and access user accounts from the dashboard.
High availability and disaster recovery for the BlackBerry Infrastructure and BlackBerry UEM Cloud environments	BlackBerry data centers are located around the world and are designed to provide high availability and disaster recovery. BlackBerry data centers provide secure physical access to buildings, monitoring, and hardware redundancies to help protect your organization’s data from natural disasters. BlackBerry data centers have disaster recovery plans for service outages. The plans are designed to have minimal impact on device users and ensure business continuity. Data and apps are backed up in near real time to avoid data loss.
Certificate-based authentication	You can send certificates to devices using certificate profiles. These profiles help to restrict access to Microsoft Exchange ActiveSync, Wi-Fi connections, or VPN connections to devices that use certificate-based authentication.

Feature	Description
Manage licenses for specific features and device controls	You can manage licenses and view detailed information for each license type, such as usage and expiration. The license types that your organization uses determine the devices and features that you can manage. You must activate licenses before you can activate devices. Free trials are available so that you can try out the service.

Key features for each device type

iOS devices

Feature	Description
Run app lock mode	On iOS devices that are supervised using Apple Configurator 2, you can use an app lock mode profile to limit the device to run only one app. For example, you can limit access to a single app for training purposes or for point-of-sales demonstrations.
Device activation	You can use Apple Configurator 2 to prepare devices for activation in BlackBerry UEM. Users can activate the prepared devices without using the BlackBerry UEM Client app.
Filter web content	You can use web content filter profiles to limit the websites that a user can view on a device. You can enable automatic filtering with the option to allow and restrict websites, or allow access only to specific websites.
Link Apple VPP accounts to a BlackBerry UEM domain	The Volume Purchase Program (VPP) allows you to buy and distribute iOS apps in bulk. You can link Apple VPP accounts to a BlackBerry UEM domain so that you can distribute purchased licenses for iOS apps associated with the VPP accounts.
Apple Device Enrollment Program	You can configure BlackBerry UEM to use the Apple Device Enrollment Program (DEP) so that you can synchronize BlackBerry UEM with the DEP. After you configure BlackBerry UEM, you can use the BlackBerry UEM management console to manage the activation of the iOS devices that your organization purchased for the DEP. You can use multiple DEP accounts. You can link multiple Apple DEP accounts to one BlackBerry UEM domain.
Support for app-based PKI solutions	Added support for app-based PKI solutions, such as Purebred, which can enroll certificates for BlackBerry Dynamics apps. You can now install the PKI app on devices and allow the latest versions of BlackBerry Dynamics apps, such as BlackBerry Work and BlackBerry Access, to use certificates enrolled through the PKI app.
Use custom payload profiles	You can use custom payload profiles to control features on iOS devices that are not controlled by existing BlackBerry UEM policies or profiles. You can create Apple configuration profiles using Apple Configurator and add them to BlackBerry UEM custom payload profiles. You can assign the custom payload profiles to users, user groups, and device groups.
BlackBerry Secure Gateway	The BlackBerry Secure Gateway allows iOS devices with the MDM controls activation type to connect to your work email server through the BlackBerry Infrastructure and BlackBerry UEM. If you use the BlackBerry Secure Gateway, you don't have to expose your mail server outside of the firewall to allow users with these devices to receive work email when they are not connected to your organization's VPN or work Wi-Fi network.

Feature	Description
Integration with BlackBerry Dynamics	You can use the BlackBerry Dynamics profile to allow iOS devices to access BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. You can assign the BlackBerry Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps. The profile allows you to enable BlackBerry Dynamics for users that are not already BlackBerry Dynamics enabled.
Per-app VPN	You can set up per-app VPN for iOS devices to specify which apps on devices must use a VPN for their data in transit. Per-app VPN helps decrease the load on your organization's VPN by enabling only certain work traffic to use the VPN (for example, accessing application servers or webpages behind the firewall). This feature also supports user privacy and increases connection speed for personal apps by not sending the personal traffic through the VPN. For iOS devices, apps are associated with a VPN profile when you assign the app or app group to a user, user group, or device group.
Apple Activation Lock	The Activation Lock feature requires the user's Apple ID and password before a user can turn off Find My iPhone, erase the device, or reactivate and use the device. You can bypass the activation lock to give a COPE or COBO device to a different user.
Personal app lists	You can view a list of apps that are installed in a user's personal space on iOS devices in your environment. You can view a list of personal apps installed on a user's device on the User Details page or view a list of all personal apps installed in users' personal spaces on the Personal apps page in the management console.
Lost Mode for supervised iOS devices	Lost Mode allows you to lock a device, set a message that you want to display, and view the current location of the lost device. You can enable Lost Mode for supervised iOS devices.
IBM Notes Traveler support	iOS devices can connect to IBM Notes Traveler through the BlackBerry Secure Gateway.
Face ID support	BlackBerry UEM supports Face ID for device authentication and to open BlackBerry Dynamics apps.
Shared device management	You can allow multiple users to share an iOS device. You can customize terms of use that users must accept to check out shared devices. A user can check out a device using local authentication and when they are done using it, they can check it in and the device is available for the next user. Shared devices remain managed by BlackBerry UEM during the check-out and check-in process. This feature was designed for supervised devices with the following configuration: • App lock mode enabled • VPP apps assigned

Android devices

Feature	Description
Manage Android Enterprise devices	You can activate Android devices to use Android Enterprise, which is a feature developed by Google that provides additional security for organizations that want to manage Android devices and allow their data and apps on Android devices. Devices can be activated to have only a work profile, or to have both work and personal profiles. You can have full control over both profiles and have the ability to wipe the entire device, or you can allow user privacy for the personal profile and only have the ability to wipe work data from the device. Samsung and BlackBerry powered by Android devices offer additional administrator options, including an enhanced set of IT policy rules, when activated with Android Enterprise Customers who have configured BlackBerry UEM to manage Google Play accounts can now migrate Android Enterprise devices from an on-premises BlackBerry UEM server to UEM Cloud or another on-premises BlackBerry UEM server.
Work and personal – full control activations for Android Enterprise devices	This activation type is for devices running Android 8 and later. It lets you manage the entire device. It creates 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. Data in both the work and personal profiles is protected using encryption and a method of authentication such as a password.
Manage devices using Knox MDM and Knox Workspace	BlackBerry UEM can also manage Samsung devices using Samsung Knox MDM and Samsung Knox Workspace. Knox Workspace provides an encrypted, password-protected container on a Samsung device that includes your work apps and data. It separates a user's personal apps and data from your organization's apps and data and protects your apps and data using enhanced security and management capabilities that Samsung developed. When a device is activated, BlackBerry UEM automatically identifies whether the device supports Knox. In addition to the standard Android management capabilities, BlackBerry UEM includes the following management capabilities for devices that support Knox: • An enhanced set of IT policy rules • Enhanced application management including silent app installations and uninstallations, silent uninstallations of restricted apps, and prohibitions to installing restricted apps • App lock mode For more information about supported devices, see the Compatibility matrix. For more information about Knox, visit https://www.samsungknox.com.

Feature	Description
Integration with BlackBerry Dynamics	You can use the BlackBerry Dynamics profile to allow Android devices to access BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. You can assign the BlackBerry Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps. The profile allows you to enable BlackBerry Dynamics for users that are not already BlackBerry Dynamics enabled.
Per-app VPN	You can enable per-app VPN for Android devices that have a work profile to restrict the use of BlackBerry Secure Connect Plus to specific work space apps that you add to an allowed list.
Zero-touch enrollment	BlackBerry UEM supports devices running Android 8.0 or later that have been enabled for zero-touch enrollment. Zero-touch enrollment offers a seamless deployment method for organization-owned Android devices making large-scale device deployment fast, easy, and secure for the organization and employees. Zero-touch enrollment makes it simple for IT administrators to configure devices online and have enforced management ready when employees receive their devices. See the information from Google: Zero-touch enrollment management, and the zero-touch enrollment overview information. You can get started with zero-touch enrollment in just a few steps: purchase devices, assign the devices to users, configure policies for your organization, and deploy the devices to users. You need to work with your reseller or carrier to get access to the Zero-touch portal and get devices configured in the portal.
Support for app-based PKI solutions	Support for app-based PKI solutions, such as Purebred, which can enroll certificates for BlackBerry Dynamics apps. You can install the PKI app on devices and allow the latest versions of BlackBerry Dynamics apps, such as BlackBerry Work and BlackBerry Access, to use certificates enrolled through the PKI app.
Android SafetyNet	When administrators enable Android SafetyNet attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of Android devices that have been activated with the Android Enterprise, Samsung Knox, and MDM controls activation types in your organization's environment.
Security patch level enforcement for BlackBerry Dynamics apps	You can apply security patch level enforcement to BlackBerry Dynamics apps. If the security patch level is not met, you can choose to delete the BlackBerry Dynamics app data, not allow BlackBerry Dynamics apps to run on the device, or perform no actions on the device.
Derived smart credentials	Use Entrust IdentityGuard derived smart credentials for signing, encryption, and authentication for BlackBerry Dynamics apps and apps in the work space on Android Enterprise and Samsung Knox Workspace devices.
Factory reset protection for Android Enterprise devices	You can set up a Factory reset protection profile for your organization’s Android Enterprise devices that have been activated using the Work space only activation type. This profile allows you to specify a user account that can be used to unlock a device after it has been reset to factory settings or remove the need to sign in after the device has been reset to factory settings.

Windows 10 devices

Feature	Description
Support for Windows 10 devices	You can manage Windows 10 devices, including Windows 10 Mobile devices and Windows 10 tablets and computers.
Proxy support for Windows 10 devices	You can configure VPN and Wi-Fi work connections for Windows 10 devices and you can set up a proxy server as part of the Wi-Fi profile for Windows 10 Mobile devices.
Per-app VPN	You can set up per-app VPN for Windows 10 devices to specify which apps on devices must use a VPN for their data in transit. Per-app VPN helps decrease the load on your organization's VPN by enabling only certain work traffic to use the VPN (for example, accessing application servers or webpages behind the firewall). This feature also supports user privacy and increases connection speed for personal apps by not sending the personal traffic through the VPN. For Windows 10 devices, apps are added to the app trigger list in the VPN profile.
Windows Information Protection for Windows 10 devices	You can configure Windows Information Protection profiles to separate personal and work data on devices, prevent users from sharing work data outside of protected work apps or with people outside your organization, and audit inappropriate data sharing practices. You can specify which apps are protected and trusted to create and access work files.
Whitelist antivirus vendors	In the compliance profile, in the "Antivirus status" rule for Windows devices, you can choose to allow antivirus software from any vendor, or allow only those that you added to the "Allowed antivirus vendors" list. The rule will be enforced if a device has antivirus software enabled from any vendor that is not whitelisted.
Azure Active Directory Join	BlackBerry UEM supports Azure Active Directory Join which allows a simplified MDM enrollment process for Windows 10 devices. Users can enroll their devices with BlackBerry UEM using their Azure Active Directory username and password. Azure Active Directory Join is also required to support Windows AutoPilot, which allows Windows 10 devices to be automatically activated with BlackBerry UEM during the Windows 10 out-of-box setup experience. **Note**: To enable automatic MDM enrollment with BlackBerry UEM during the Windows 10 out-of-box setup, a BlackBerry UEM certificate must be installed on the device.

BlackBerry 10 devices

Feature	Description
Manage work information separately on a BlackBerry 10 device	BlackBerry Balance technology makes sure that personal and work information and apps are separated on BlackBerry 10 devices. It creates a personal space and a work space and provides full management of the work space. For government and regulated industries that want to lock the device down further, additional options include full control over the work space and some control over the personal space, or you can create only a work space on the device to give your organization full control over the device.

Compatibility and requirements

You can find up-to-date information about compatibility, including device types, operating systems for devices, and browsers for accessing BlackBerry UEM, in the BlackBerry UEM Compatibility Matrixes.

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada