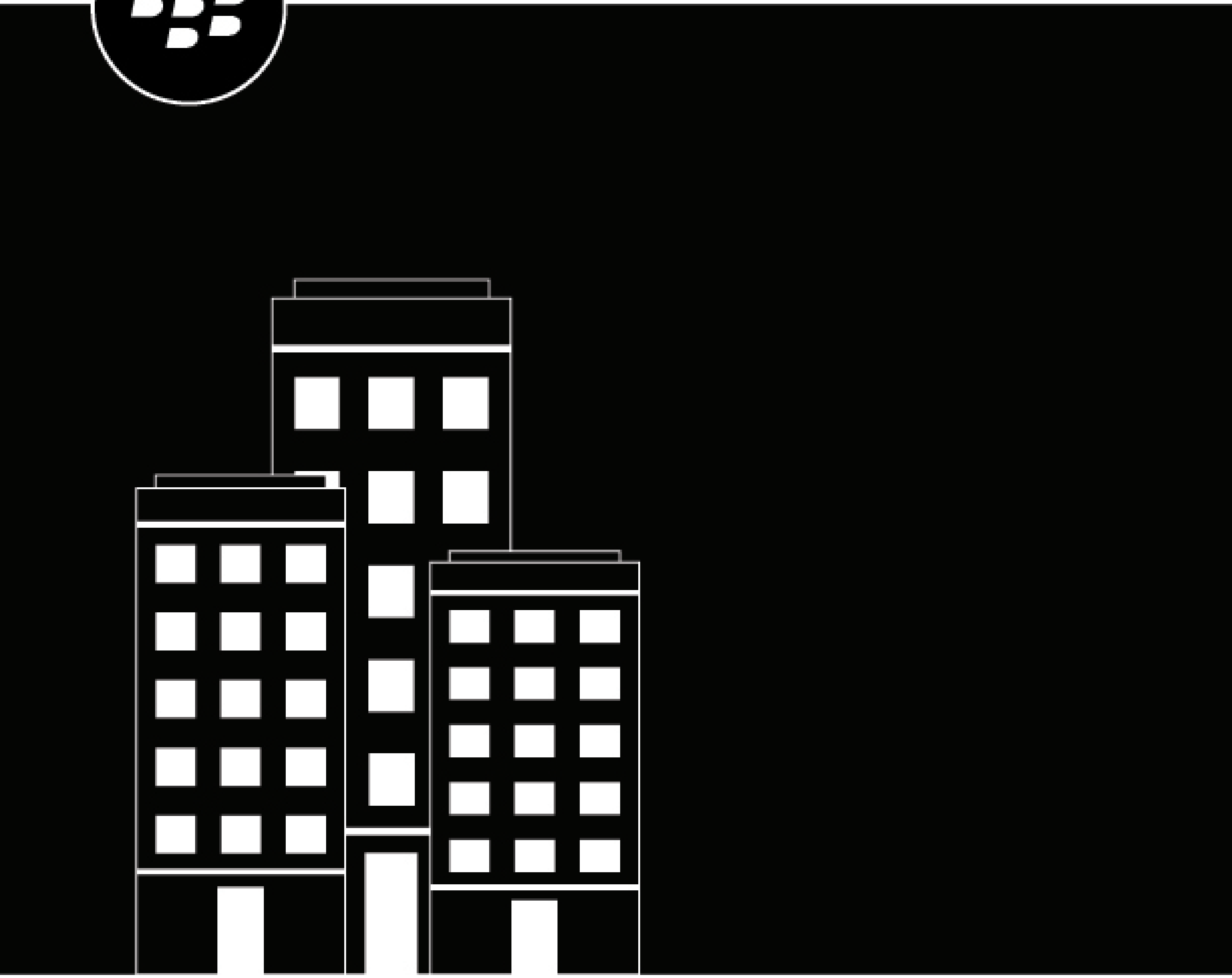

BlackBerry UEM

Release Notes

12.12.1

Contents

Installing the software

You can use the setup application to install BlackBerry UEM version 12.12, or to upgrade from 12.10.x or 12.11.x. When you upgrade the software, the setup application stops and starts all the BlackBerry UEM services for you. The BlackBerry UEM setup application backs up the database by default.

Note: As of BlackBerry UEM release 12.10, JRE is no longer bundled with the installer. If you are installing BlackBerry UEM, you must first download and install JRE (minimum version JRE 8u151).

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

Fixed issues

Fixed issues in BlackBerry UEM 12.12.1a quick fix 3

Management console fixed issues

On the Android tab of the VPN profile page, a new "Connection type" list allows you to specify the connection type that Android devices use for a VPN gateway. (EMM-143143) You can select one of the following: • Keep on: Starting or stopping a VPN connection does not depend on starting or stopping apps. This is the default value. • On demand: Starting or stopping a VPN connection depends on starting or stopping apps.
After you upgraded BlackBerry UEM, a user with the Junior HelpDesk role could not set an activation password. (EMM-142625)

Fixed issues in BlackBerry UEM 12.12.1a quick fix 2

User and device management fixed issues

The Root MDM Verification certificate was being built and delivered to iOS devices before the certificate was generated and inserted into the database. (EMM-143897)
If the Root MDM Verification certificate was removed from a device, the BlackBerry UEM Core did not resend the certificate to the device after a restart. (EMM-142368)
When an iOS 13 device was configured to use the BlackBerry Secure Gateway, if you activated the device and it tried to connect to the BlackBerry Secure Gateway before it received the CA certificate, a "Cannot Verify Server Identity" message displayed on the device. (EMM-132628)

Management console fixed issues

You couldn't view the "Device.compromised.state.reason" in log files without selecting the "Enable MDM payload logging" option in Settings > Infrastructure > Logging. (EMM-141578)

Fixed issues in BlackBerry UEM 12.12.1a quick fix 1

Management console fixed issues

Junior and Senior Helpdesk administrators received an error when opening a user account. (EMM-142575)

On the managed devices page, an Android device might have displayed multiple times for the same user. (EMM-142574)
BlackBerry UEM Cloud could not reconcile URL format changes and successfully connect to VPP servers. (EMM-142302)
VPP account removal sometimes failed. (EMM-141084)

Fixed issues in BlackBerry UEM 12.12 MR1

User and device management fixed issues

On OnePlus and Redmi devices, in certain circumstances, BlackBerry Dynamics apps could get stuck in an authentication loop. (FIRST-17108)

Management console fixed issues

If an administrator restricted versions of a BlackBerry Dynamics app using the BlackBerry UEM management console, the way the restricted version number was processed may have unintentionally blocked more versions of the app than intended. (FIRST-17124)
If you were using an LDAP connection to an Active Directory environment and you made a change to a user's attributes such as the email address, the change would not synchronize with UEM. (EMM-136693)
BlackBerry Dynamics-hosted .apk files were not installed on devices if the activation profile was enabled for Google Play. (EMM-137637)
When you edited an app configuration for a hosted app, a duplicate app configuration might have been created. (EMM-137108)
iOS device users were not able to access apps and sites without using their credentials after an administrator assigned a SCEP profile and a single-sign on profile to them. (EMM-137085)
The compliance violations list in the management console might have been empty for apps that were built using newer SDKs. (GD-47035)

BlackBerry Secure Connect Plus fixed issues

In an environment that used BlackBerry Secure Connect Plus with Samsung Knox devices, if the environment blocked the *.secb2b.com call from UEM, the KNOX (KLM/ELM) license might have expired. (EMM-140039)

Fixed issues in BlackBerry UEM 12.12.0 quick fix 1

Management console fixed issues

The Apple DEP devices page now loads correctly in the management console. (EMM-138323)

Fixed issues in BlackBerry UEM 12.12.0

Installation, upgrade, and migration fixed issues

If you applied an IT policy pack on your organization's BlackBerry UEM 12.10 MR1 server and you upgraded to BlackBerry UEM 12.11, the new IT policies were not hidden even though the policy pack was installed on the BlackBerry UEM 12.10 MR1 server. (EMM-129252)
You could not upgrade from UEM 12.9 to UEM 12.11 if the directory path contained brackets. For example, C:\Program Files (EXAMPLE)\BlackBerry\UEM\. (EMM-126340)

User and device management fixed issues

If you modified an existing app lock mode profile for a Samsung Knox device, the updated profile was not correctly updated on the device. (EMM-131626)
You could not modify and save an enterprise connectivity profile that had iOS VPN on demand rules configured. (EMM-132378)
iOS DEP devices could not authenticate with BlackBerry UEM during activation if the password contained special characters such as £. (EMM-126396)

Management console fixed issues

You could not save a BlackBerry Dynamics entitlement after you changed the app configuration ranking. (EMM-135823)
In the BlackBerry Dynamics profile, the Android biometrics options mentioned 'fingerprint' only. However, Android device users could use their preferred biometric setting, rather than being confined to just fingerprint identification. (EMM-135519)
In the Apps section of the BlackBerry UEM management console, if you selected an app category and then performed a search on the filtered results, after the search the app categories no longer displayed. (EMM-130581)
When a DEP connection failed because a new token was generated on the Apple DEP portal, you did not receive an event notification email message. (EMM-126723)
You could save an iOS app shortcut that had a space in the URL. (EMM-126319)

When you clicked Managed devices or All users, selected a user, resized the window, and clicked the back arrow, the screen that displayed was empty. (EMM-125716)
A warning message did not display when you created an activation profile for an Android device and you did not select an activation type. (EMM-123636)
If you scheduled a directory synchronization job for offboarding Microsoft Active Directory users, the synchronization job might have failed. (EMM-116146)

Known issues in BlackBerry UEM 12.12

Items marked with an asterisk (*) are new for this release.

Installation, upgrade, and migration known issues

* The ITPolicyKeyMapping user table is not removed from the database during a BlackBerry UEM upgrade. (EMM-143254)

Workaround: Manually remove the ITPolicyKeyMapping table from the database before upgrading BlackBerry UEM.

When you migrate BlackBerry Work from a Good Control server to a BlackBerry UEM 12.12 server, upgrade the server to version 12.12 MR1, and then migrate the app again to another BlackBerry UEM 12.12 MR1 server, the migration might fail. (GD-49189)

Workaround: Re-activate the app on the destination server.

When you migrate a BlackBerry Dynamics app, that was built using a version of the BlackBerry Dynamics SDK earlier than 7.1, from one BlackBerry UEM server to another BlackBerry UEM server, the app will begin migration but when the user opens the app, a 'Migration failed' message is displayed. (EMM-141581)

Workaround: Uninstall the app from the device.

BlackBerry UEM does not block DEP devices that do not have the BlackBerry UEM Client or BlackBerry Dynamics apps activated. (EMM-141410)

Workaround: Reactivate the device on the destination server.

After you upgrade from BlackBerry UEM 12.11 to BlackBerry UEM 12.12, or install a new instance of BlackBerry UEM 12.12, you cannot use a Cisco ISE API solution to enhance the security management of network devices. (EMM-141132)

Workaround: Copy commons-collections-3.2.2 in :\C\Program Files\BlackBerry\UEM\ui\lib\runtime, paste it into :\C\Program Files\BlackBerry\UEM\Core\tomcat-core\lib, and restart the BlackBerry UEM Core.

You cannot migrate a BlackBerry Dynamics-enabled BlackBerry UEM Client on a device that has been activated using the 'Work and personal - full control (Samsung Knox)', or 'Work space only - (Samsung Knox)' activation types. (EMM-140909)

When you migrate a Good Control policy set to BlackBerry UEM 12.12 MR1, if the 'Checks Antivirus Status' is set to Disabled, after the migration completes, the corresponding 'Antivirus Status' option is enabled in the compliance policy. (EMM-140859)

Workaround: In the migrated compliance policy, change the 'Enforcement action for BlackBerry Dynamics apps' option to 'Monitor and log'.

You cannot migrate a Good Control policy set to BlackBerry UEM 12.12 MR1, if the 'Allow all Hardware Models' option is set to No, and you haven't selected any options for 'Permitted Hardware Models'. (EMM-140845)

After you upgrade to BlackBerry UEM 12.12 MR1, compliance profiles are not upgraded to the latest user interface. (EMM-140825)

Workaround: After upgrading, wait 10 minutes before logging in to the console.

When you migrate BlackBerry Dynamics users and their iOS devices to BlackBerry UEM 12.12 MR1, if you have configured an APNs certificate on the source server but not on the destination server, the device is placed in the 'devices will be migrated' table. (EMM-140700) **Workaround**: Configure APNs certificates on the destination server before migrating devices.
You cannot delete a user from a source server after migrating their device. (EMM-140678) **Workaround**: Remove or replace the activation profile for the user on the source server and then delete the user.
A non-authentication delegate BlackBerry Dynamics app is marked as 'migration completed' after the migration process for a non-authentication delegate BlackBerry UEM Client app starts. (EMM-140138)
The BlackBerry Secure Connect Service might not start after a software upgrade. (EMM-137170) **Workaround**: Perform the upgrade again.
When you install the BlackBerry Workspaces plug-in with BlackBerry UEM, the next time you open the UEM management console, an error message appears even though BlackBerry UEM and BlackBerry Workspaces are behaving as expected. (SNP-561) **Workaround:** Dismiss the error message. It does not reappear.

User and device management known issues

Note that some of these issues are for the BlackBerry UEM Client and will be fixed in a future BlackBerry UEM Client release.

* Easy activation of BlackBerry Dynamics apps might fail on new iOS devices. (EMM-143135)
A S/MIME certificate might be removed from a device after the user has installed it. (EMM-141529) **Workaround**: Reinstall the certificate.
The BlackBerry UEM Core does not send the Device IMEI value to the Lookout for Work app when the app activates. (EMM-140895)
During SCEP enrollment, BlackBerry UEM might not be able to the retrieve the challenge password that the device uses for certificate enrollment. (EMM-140361)
You cannot remove apps from a user on the 'Assigned to <x> users' tab. (EMM-136286) **Workaround**: Go to the user's page and delete the app.
Certificates from a two-key pair Entrust profile can't be installed on an iOS device. (EMM-120349)
On an Android 9 device, if the Prevent Screen Capture security policy setting is disabled, the user can cut/copy/share data from a BlackBerry Dynamics app to a non-BlackBerry Dynamics app, even when data leakage prevention (DLP) is enabled via Pixel Launcher functionality. To ensure no data leakage, it is recommended that you enable the Prevent Screen Capture policy setting. (GD-36449)
You can't use the Purebred app and Entrust smart credentials at the same time on iOS devices with BlackBerry Dynamics. If you do, the Purebred certificate is imported on the incorrect user credential profile. (EMA-10637)

If your organization uses PKI and Entrust smart credentials together, users might need to enroll the PKI certificate multiple times on the same device (maximum of once per app). (GD-35783)

The 'Do not allow Android dictation' option in the BlackBerry Dynamics profile is used to stop dictation from keyboards, however there are certain keyboards that allow dictation through other channels. (GD-35440)

Workaround: To help mitigate the issue, you can apply an IT policy with the 'Allowed input methods' option set to 'System only' or enforce installation of particular keyboards in the Android work profile.

After an iOS user imports a certificate, the user is taken through the import process again. (G3IOS-18108)

Management console known issues

If a BlackBerry UEM administrator creates and assigns a user credential profile that is configured to use a native keystore CA connection, when a user opens a BlackBerry Dynamics app on an Android 10 device, the following error message displays: "You are required to select a personal certificate. You may need to install it if the required one is missing. Please try again." This is due to a change with the KeyChain.choosePrivateKeyAlias API in Android 10: https://issuetracker.google.com/issues/135667502

To support a native keystore connection for BlackBerry Dynamics apps on Android 10 devices, in the user credential profile, the administrator must do one of the following:

- Leave the Issuers field blank. The user will be prompted to select the certificate when it is required.
- Specify an issuer and verify that the order of the relative distinguished name complies with the required format for Android 10: For example, "CN=core2-TKCA02-CA,DC=core2,DC=sqm,DC=testnet,DC=rim,DC=net". The full distinguished name must be provided in the same order as within the target certificate. Partial names such as "DC=rim,DC=net" are not allowed.

* You cannot save a DEP enrollment configuration if you set the "Allow removal of MDM Profile" option to Off. (EMM-144491)

* On the Company directory page, the Client key field does not allow the tilde (~) character. (EMM-143686)

* If you add an internal .apk app file, select the "Publish app in Google domain" option, and select the "All Android devices" option in the "Send to" list, when you click the "Update app descriptions and details from app stores" button on the Apps page, the app is removed from user's devices. (EMM-143243)

* The app installation ranking might be ignored if the BlackBerry Work entitlement app is included in the list. (EMM-142953)

* When you configure an iOS network usage profile for apps, if one of the apps that you add includes a hyphen in the app id, after you save the profile and refresh the page, the profile displays as a blank page. (EMM-142787)

* Company directory synchronization fails when BlackBerry UEM Core detects an invalid email address for a user. (EMM-142690)

* Activation email messages generated using the BlackBerry Dynamics access key email template show <br> tags before and after the access key. (EMM-142652)

* After you upgrade BlackBerry UEM, a user with the Junior HelpDesk role cannot set an activation password. (EMM-142625)

* If you update the Autogenerated password complexity setting on the General Settings > Activation defaults page, the setting does not revert back to the default after you refresh the page. (EMM-142501)

For more information, visit support.blackberry.com/community to read article KB 62915.

* When you copy the permissions from the security administrator role to create a new administrator role, the new administrator cannot manage certificates in the BlackBerry UEM Self Service portal. (EMM-141897)

A warning icon might display next to the Apps menu item in the console, and even after you accept all the app permissions the icon might not disappear. (EMM-141702)

If your organization is using BlackBerry UEM 12.12 MR1, you cannot apply the “Allow unified account view in BlackBerry Hub” policy to Android 10 devices. (EMM-141541)

Workaround: If you need this policy enabled, contact BlackBerry support.

When you try to use the 'Change password and lock device' command in the management console for a device that was activated using an activation type, if you have configured the IT policy to use 'Numeric Complex' passwords, an error displays that states the password does not meet the minimum requirements. (EMM-141537)

Workaround: Do not use a password rule that enforces the 'Numeric Complex' option.

App configurations for BlackBerry Dynamics app do not display in the console if the name of the app configuration contains an apostrophe. (EMM-141440)

Workaround: Do not use apostrophes in app configuration names.

You might not be able to remove a VPP account that has a lot of users. (EMM-141084)

If an administrator does not have the 'View User Credential Profile' permission assigned, and you create a user credential profile to manually upload certificates, the administrator cannot upload or replace certificates. (EMM-141001)

* Some of the fields and tooltips on the Enterprise Connectivity profile page are not translated correctly into German. (EMM-140442)

The 'Tenant attestation enabled date' is updated in the database when you click Save on the Attestation page. (EMM-140416)

If you set up a service on the BlackBerry Enterprise Identity page and you select the 'Allow Kerberos Desktop ZSO when specified by authentication policy', when a user uses a browser that is not configured to use Kerberos to log in to the service, the user is directed to the UEM Self-Service portal instead of the BlackBerry Enterprise Identity log in page. (EMM-140165)

After you add a user, if you click the 'View activation email' link on the user's summary page, close the page, and click the link again, an error might display. (EMM-139907)

In an IT policy for Android devices, the tooltip for the 'Apps allowed to access external storage' option states that the option can be applied to devices activated using the 'Work space only (Premium)' activation type but it cannot. (EMM-138293)

A message does not display in the console when a BlackBerry Dynamics connectivity verification compliance violation occurs. (EMM-137201)

A per-app VPN connection cannot be established on a device that is activated with the 'User privacy – User enrollment' activation type. (EMM-136964)

The BlackBerry Connectivity app might not be delivered to an Android device that has been activated using the 'Work and personal - user privacy (Samsung Knox)' activation type and 'Google Play app management for Samsung Knox Workspace devices' is enabled. (EMM-136648)

Workaround: Assign the .apk file to the device as an internal app and select the "Publish app in Google domain" option.

On the device tab, if you try to upgrade the software version on a supervised iOS device to a specific version number, when you click on Download and install, the OS is downloaded but not installed. Ticket FB7453536 was raised with Apple. (EMM-135440)

When you add an internal app and an icon for the app, if you click the Refresh button on the Apps page, the icon does not display in the list of apps. (EMM-134638)

Apps do not get unblocked after adding a corresponding version to *my*Account and synchronizing the app with BlackBerry UEM. (GD-45067)

When you are using the Advanced view in the management console, the device details page displays the incorrect Total internal storage amount for devices. (EMM-98304)

You can't update the version of an app in the BlackBerry UEM console before the newer version of the app is available in Google Play. (EMM-89974)

Workaround: Add the new version of the app to Google Play, wait for Google to publish the app and then add the app to the BlackBerry UEM console

BlackBerry Secure Connect Plus known issues

After you upgrade to BlackBerry UEM 12.12, the BlackBerry Secure Connect Plus service might not start and stay running if syslog is configured for localhost. (EMM-139980)

Workaround: Change the syslog configuration to connect to another server, or connect to 127.0.0.1 instead of "localhost".

UEM Self-Service known issues

The expiration period for access keys generated in UEM Self-Service is 24 hours instead of 30 days. (EMM-78769)

BlackBerry Web Services known issues

* When using the API, the set or place a certificate for a profile assigned to user request returns a "No certificate password specified in the request body" error, even if the password is provided. (EMM-140843)

Legal notice

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada