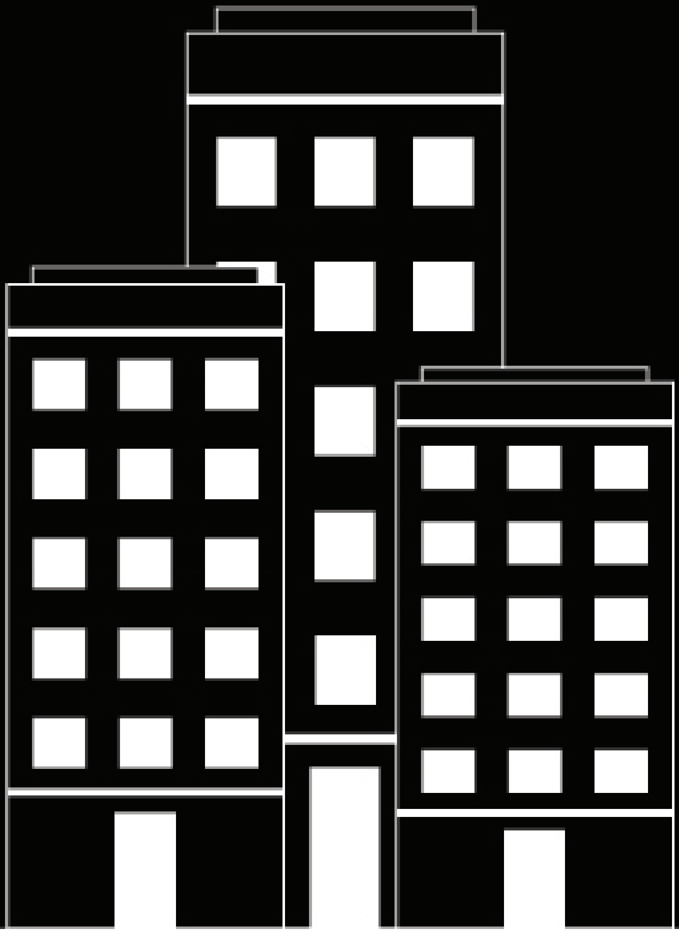

BlackBerry UEM

Release Notes

12.11

Contents

Installing the software

You can use the setup application to install BlackBerry UEM version 12.11 MR1 or to upgrade from 12.9.x or 12.10.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.

IMPORTANT: 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 12.11 MR1

BlackBerry Intelligent Security

- **BlackBerry Intelligent Security**: BlackBerry UEM supports BlackBerry Intelligent Security. For more information, see the documentation here.

Android

- **Apply security patch level enforcement to BlackBerry Dynamics apps on Android devices**: In a compliance profile 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.
- **Compliance policy update**: A new compliance setting allows administrators to enable or disable anti-debugging for BlackBerry Dynamics apps. If your organization prohibits turning off detection for rooted OS or failed attestation, you can use this setting to disable the anti-debugging check without disabling rooted OS or failed attestation detection.
- **User notifications**: Updates to Android 10 required changes to the BlackBerry UEM Client to use notifications instead of pop-up dialog boxes to inform users of events and request user input. Users must allow notifications from the UEM Client to avoid unexpected behavior.
- **UEM Client native library updates:** The BlackBerry UEM Client for Android native libraries have been updated to support a 64-bit architecture.
- **BlackBerry Connectivity native library updates:** The BlackBerry Connectivity app for Android native libraries have been updated to support a 64-bit architecture.

iOS

- **Compliance policy update**: A new compliance setting allows administrators to enable or disable anti-debugging for BlackBerry Dynamics apps. If your organization prohibits turning off Jailbreak OS detection, you can use this setting to disable the anti-debugging check without Jailbreak OS detection.
- **iOS 13 support**: BlackBerry UEM now supports iOS 13.

  For more information about the supported operating systems, see the Mobile/Desktop OS and Enterprise Applications compatibility matrix.

Samsung Knox

- **Common criteria mode**: In an IT policy, you can put Samsung Knox devices into Common Criteria mode.

MDM Controls activation type

- **MDM Controls activation type is not required for BBM Enterprise activation**: Administrators are no longer required to ensure that MDM Controls is an allowed activation type to successfully activate BBM Enterprise.
- **MDM Controls activation type is deprecated for Android 10 devices:** You should activate Android devices using the “Android Enterprise” activation types. You can use device groups and compliance profiles to manage what happens for devices activated with "MDM controls" that are updated to Android 10. You can set the "Android 10 device activated with MDM Controls" event notification so you can be notified when an Android 9 device with MDM Controls is upgraded to Android 10 and can no longer be properly managed. For more information about the deprecation of the MDM Controls activation type, visit support.blackberry.com/community to read article 48386.

SHA1

- BlackBerry UEM 12.11 is the last BlackBerry UEM release that supports SHA1.

APNs

- **APNs API update**: BlackBerry UEM now communicates with APNs using the HTTP/2 APNs API.

IT Policy Rule updates

iOS	Allow QuickPath keyboard (supervised only)
iOS	Allow Wi-Fi to be disabled (supervised only)
iOS	Allow finding devices in the Find My app (supervised only)
iOS	Allow finding friends in the Find My app (supervised only)
Android Global (Samsung Knox devices only)	Enable Common Criteria mode

Whats new in BlackBerry UEM 12.11

Security

- **iOS app integrity check**: You can use the iOS app integrity check framework to check the integrity of iOS work apps that have been published to the App Store. This feature uses Apple DeviceCheck and other methods to provide a way to identify that your app is running on a valid Apple device and that the app is published by the specified Apple Team ID. For more information on Apple DeviceCheck, see the information from Apple. This setting applies only to devices running iOS 11 and later. Activation of BlackBerry Dynamics apps that were built using BlackBerry Dynamics SDK for iOS version 5.0 or earlier will fail if you enable the ‘Perform app integrity check on BlackBerry Dynamics app activation’ option in the activation profile and if you add those apps for iOS app integrity check. If a BlackBerry Dynamics app that was built using BlackBerry Dynamics SDK for iOS version 5.0 or earlier is already activated, and you select the 'Perform periodic app integrity checks' option in the Activation profile, the app will fail the periodic attestation check and the device will be subject to the enforcement action specified in the compliance profile that is assigned to the user.

  Note: You cannot enable the iOS app integrity checking on enterprise apps that your organization has developed and distributed internally using the Apple Enterprise Distribution program.

Management Console

- **BlackBerry Dynamics Connectivity profile change**: The Route All option has been replaced with a Default Route option in the BlackBerry Dynamics Connectivity profile allowing for more detailed control over how BlackBerry Dynamics apps built using the latest BlackBerry Dynamics SDK can connect to app servers. This allows you to configure rules to avoid double tunneling the UEM App Store and UEM hosted application push.
- **BlackBerry Dynamics access keys**: You can now generate BlackBerry Dynamics access keys for users that do not have an email address.
- **Notifications for changes to Android Enterprise apps**: Administrators can now receive notifications when the status of an Android Enterprise app on Google Play has changed and requires review. When an app requires review, UEM marks the apps listed on the Apps screen. Administrators can apply a filter to easily see the apps that need to be reviewed or approved and take the appropriate action. From the Settings > Event notifications menu, you can set the types of events that you want administrators to be notified about. For example, you can notify administrators if an app requires review if changes were made to the app’s availability, version, approval status, permissions, app configuration schemas, or if an app was not successfully installed on a user’s device.
- **Whitelist antivirus vendors for Windows devices**: In the compliance profile, in the “Antivirus status” rule for Windows devices, you can now 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.
- **User credential profiles support using Entrust for BlackBerry Dynamics apps**: You can now use your Entrust PKI connection to enroll certificates for BlackBerry Dynamics apps using the User credential profile.
- **Compliance violation reporting**: When a device is out of compliance, violations and any applicable actions display on the device summary page. To see which apps are in a noncompliant state, click on the ‘View noncompliant apps’ link. A device with performance alerts or compliance violations is flagged with a caution icon. Types of violations that are reported include:

  - Rooted OS or failed attestation (Android only)
  - SafetyNet attestation failure (Android only)
  - Jailbroken OS (iOS only)
  - Restricted OS version is installed (iOS, Android, macOS, Windows)
  - Restricted device model detected (iOS, Android, macOS, Windows)

  - BlackBerry Dynamics library version verification (iOS, Android, macOS, Windows)
  - BlackBerry Dynamics apps connectivity verification (iOS, Android, macOS, Windows)
  - Antivirus status (Windows only)

  In the management console, you can filter on any of the compliance rules when they occur.
- **Device compliance report**: On the dashboard, the device compliance report now includes if either the BlackBerry UEM Client or a BlackBerry Dynamics app is out of compliance.
- **Device report update**: The device report now includes the BlackBerry Dynamics compliance rule status.
- **Automatic device and OS metadata updates**: If a user activates a device with a model or OS version that is unknown to BlackBerry UEM, UEM automatically adds the new device or version metadata to the UEM database so that the metadata is available for Activation, Compliance, and Device SR profiles.
- **Enable Android keyboard restricted mode**: You can now use the ‘Enable Android keyboard restricted mode’ option in a BlackBerry Dynamics profile to force custom keyboards into incognito mode.
- **Shared device groups:** Migration is not supported for shared device groups. Users who belong to a shared device group do not appear in the Migrate users list. Devices that are part of a shared device group do not appear in the Migrate devices list.
- **New Event Notifications**: BlackBerry UEM can now email event notifications to administrators for the following events:

  - iOS VPP account expiry
  - DEP token expiry
  - IT policy pack updated
  - Metadata updated

Activation

- **Activate Android Enterprise devices without adding a Google account**: Administrators now have the option to allow Android Enterprise devices to be activated without adding a Google Play account to the workspace. You might use this option if you do not want to use Google Play to manage work apps on Android Enterprise devices or you want to activate and use the device without accessing Google services. In the activation profile, you specify whether to add Google Play to the workspace for Android Enterprise devices. By default, the activation profile adds the Google account to the work space and Google Play manages the apps. If you do not add a Google account, apps and app configurations are managed through the BlackBerry UEM infrastructure via BlackBerry UEM Client.
- **BlackBerry UEM now includes 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. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files.

  To activate a device with Work and personal – full control, the user must wipe the device and start the activation in the same way as Work space only activations.

  To enable BlackBerry Secure Connect Plus Knox Platform for Enterprise support, you must select the "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus" option in the activation profile.

  When applying IT policy rules to Android Enterprise devices with Work and personal – full control activations, the different rule categories affect different profiles on the device:

  - Global rules apply to the entire device
  - Work profile rules apply to apps and data in the work profile
  - Personal profile rules apply to apps and data in the personal profile

For example: to apply password requirements to unlock the device, use the Global password rules. To apply password requirements only to the work profile, use the Work profile password rules. To prevent screen capture only of work data, deselect the Work profile “Allow screen capture” rule and select the Personal profile “Allow screen capture” rule. To prevent screen capture of both work and personal data, deselect the Personal profile “Allow screen capture” rule.

Windows 10 Modern Management

- **Support for Azure Active Directory Join**: BlackBerry UEM now supports Azure Active Directory Join which allows a simplified MDM enrollment process for Windows 10 devices. Users can enroll their devices with UEM using their Azure Active Directory username and password.
- **Windows Autopilot support**: Azure Active Directory Join is also required to support Windows AutoPilot, which allows Windows 10 devices to be automatically activated with 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 UEM certificate must be installed on the device.

Intune

- **Microsoft Intune app protection support enhancement**: You can manage and deploy Microsoft Intune managed apps from the BlackBerry UEM management console when your environment is configured for modern authentication.

Apple Configurator

- **Enroll Apple DEP devices using Apple Configurator**: You can now use a static enrollment challenge to enroll multiple DEP devices using Apple Configurator.

BlackBerry Dynamics

- **Add public app source files as internal apps**: You can now add BlackBerry Dynamics app source files from the public app stores as internal apps so that users can install the apps without connecting to the stores.
- **Link to specific apps**: You can now send users a link or QR code that links directly to the app details page for specific BlackBerry Dynamics apps.
- **Enhancements for certificate enrollment using app-based PKI solutions**: BlackBerry UEM has simplified certificate enrollment process for app-based PKI solutions such as Purebred. To use app-based certificates with BlackBerry Dynamics apps, the "Allow BlackBerry Dynamics apps to use certificate, SCEP profiles, and user credential profiles" check box no longer needs to be selected in the BlackBerry UEM Client.

Logging

- **Logging changes:** The BlackBerry UEM administrator console includes the following changes for logging:
    - The Maximum device app audit log file size is now configured as a global setting instead of per instance. If you upgrade from a previous release, the maximum size is initially set to the minimum setting for any existing server instance.
    - Component level logging is now supported for BlackBerry Proxy Service. You can enable logging for BlackBerry Proxy Service under Settings > Infrastructure > Logging, as well as the Server group and BlackBerry Connectivity Node default settings pages.
- **Trace logging option removed:** The option to set logging level to Trace has been removed from Service logging override. You can set logging level to Info, Error, Warning, or Debug.

- **BlackBerry Proxy Service:** Component level logging is now available for BlackBerry Proxy Service. You can enable logging for BlackBerry Proxy Service on the Server group and BlackBerry Connectivity Node default settings pages.

BlackBerry Connectivity

- **BlackBerry Connectivity app updates**: The BlackBerry Connectivity app (version 1.18.0.811) for Samsung Knox Workspace and Android Enterprise devices does not include fixes or improvements, but is upversioned so that administrators can assign and update the app on devices. If enterprise connectivity is required, you are now required to use the BlackBerry UEM administrator console to add the BlackBerry Connectivity app as an internal app and assign it (with a Required disposition) to Samsung Knox Workspace and Android Enterprise devices that don't have access to Google Play. For more information, visit support.blackberry.com/community to read article 37299.

BlackBerry Web Services

- **Enabling access to the BlackBerry Web Services over the BlackBerry Infrastructure**: If a web service client is outside of your organization's firewall and it requires access to the BlackBerry Web Services APIs (REST or legacy SOAP), the client can connect to the APIs securely over the BlackBerry Infrastructure. For more information, see the Getting started page in the REST API reference and the "Access On-Premise UEM web service securely" example.

  A UEM administrator must explicitly enable access to the BlackBerry Web Services APIs over the BlackBerry Infrastructure. An administrator can enable or disable this access in the management console in Settings > General settings > BlackBerry Web Services access.

Changes to the Planning and the Installation and Upgrade content

Documentation changes:The Planning and the Installation and Upgrade content have been reorganized for BlackBerry UEM version 12.11. The major changes are:

- A new "Preinstallation and preupgrade requirements" section in the Planning content consolidates information that was previously in several places in the Installation content. Most notably, the Preinstallation and preupgrade checklist has been removed from the Installation content and forms part of the new section.
- Information about ports has moved to the Planning content.
- Overview information about high availability has been consolidated into the Planning content. It was previously in the Installation content and the Configuration content.

New IT policy rules

iOS

Allow Bluetooth (supervised only)	Specify whether users can use Bluetooth on the device. If you don't want to allow Bluetooth, the "Allow Bluetooth changes" rule should also not be selected. If "Allow Bluetooth changes" is selected, users can re-enable Bluetooth on the device.
Allow modifying personal hotspot settings (supervised only)	Specify whether the user can to modify the personal hotspot settings.
Allow sending Siri logs to Apple	Specify whether the device can send Siri logs to Apple servers.

Android Enterprise (Global)

Allow users to deactivate devices from UEM Client	Specify whether the user can deactivate the device using the BlackBerry UEM Client. If this rule is not selected, the Deactivate My Device button in the BlackBerry UEM Client is disabled.

Android Enterprise (Work profile)

Allow Android system windows	Specify whether Android devices can display windows other than app windows; for example, windows for toasts, system error messages, and phone calls.
Allow users to modify apps in Android Settings	Specify whether users can modify apps in Settings or launchers. If this rule is not selected, users can't uninstall apps, disable apps, clear app caches, clear app data, force apps to stop, or clear app defaults from the device Settings or launchers.
Allow system error dialogs	Specify whether system error dialogs for crashed or unresponsive apps display on the device. If this rule is not selected, when an app stops or is unresponsive, the system will force-stop the app as if the user chose the "close app" option in the dialog box. A feedback report isn't collected because users can't provide explicit consent.
Skip first use hints	Specify whether work apps should to skip showing any introductory hints that display the first time the app is launched.

Android Enterprise (Personal profile)

Allow screen capture	Specify if a user can take screen shots of the device.
Allow autofill	Specify whether the device can save user-entered form data to automatically fill future forms.
Allow adding and removing accounts	Specify whether a user can add or remove accounts, such as email accounts, on the device.
Allow additional Google accounts	Specify whether the user can add additional Google accounts to the work space.

Disallowed account types	Specify the types of accounts that cannot be added to the work space. If no account types are specified, there is no restriction. Disallowing an account type blocks users and apps from adding the account. Account types are defined by the app that uses the account and so can't be thoroughly documented here. Some useful examples are: • BlackBerry Hub email: com.blackberry.email.unified • BlackBerry Hub CalDAV: com.blackberry.dav.caldav • BlackBerry Hub CardDAV: com.blackberry.dav.carddav • Microsoft Outlook: com.microsoft.office.outlook.USER_ACCOUNT • Gmail ActivSync: com.google.android.gm.exchange • Gmail POP3: com.google.android.gm.pop3 • Gmail IMAP: com.google.android.gm.legacyimap • Google user account: com.google • LinkedIn: com.linkedin.android For more information, visit support.blackberry.com/community to read article 46860.
Allow lock screen features	Specify whether special features can be enabled on the device lock screen.
Allow camera on lock screen	Specify whether users can access the device camera on lock screen.
Allow notifications	Specify whether the device can display notifications on the lock screen.
Allow all notification content	Specify whether all notification content can appear on the lock screen or only the notification type.
Allow fingerprint authentication	Specify whether the user can unlock the device using a fingerprint.
Allow trust agents	Specify whether trust agents can unlock the device.
Allow NFC trust agent	Specify if NFC can be used to unlock the device.
Allow tags with basic authentication to unlock the device	Specify if NFC tags that authenticate using the tag ID can be used to unlock the device.
Allow secure NFC tags to unlock the device	Specify if NFC tags that use challenge-response authentication can be used to unlock the device.
Allow Bluetooth trust agent	Specify if Bluetooth can be used to unlock the device.
Allow places trust agent	Specify if places can be used to unlock the device.
Allow custom places	Specify if a user can trust places other than Home.
Allow Face trust agent	Specify if face image can be used to unlock the device.
Allow Voice trust agent	Specify if voice can be used to unlock the device.
Allow On-body trust agent	Specify if On-body can be used to unlock the device.

Trust agent inactivity timeout	Specify Device inactivity timeout in minutes. When a device is in an idle state for a certain period of time, trust agents will be revoked.
Allow installation of non Google Play apps	Specify whether a user can install apps using the app installer (the ACTION_INSTALL_PACKAGE mechanism).
Allow developer options	For work space only devices, specify whether users can enable developer options on the device. For Work and personal - user privacy devices, the option for users to turn on developer options can't be disabled. If this rule is not selected the device deletes any apps that aren't on the app list in UEM that users have installed to the work profile using the developer options.

Fixed issues

Fixed issues in BlackBerry UEM 12.11.1 quick fix 4

This release contains bug fixes.

Fixed issues in BlackBerry UEM 12.11.1 quick fix 3

BlackBerry UEM Core was unable to connect to VPP servers. (EMM-142302)
You could not view the 'Device.compromised.state.reason' in log files without selecting the 'Enable MDM payload logging' option in Settings > Infrastructure > Logging. (EMM-141578)
After you created a VPN profile for Juniper Pulse Secure, when the profile was sent to the device, some of the fields were missing. (EMM-140846)

Fixed issues in BlackBerry UEM 12.11.1 quick fix 2

In BlackBerry Web Services for BlackBerry UEM, the ContainerID is returned in the CreateAccessKey API. (EMM-137643)
VPP account removal sometimes failed. (EMM-137061)
Errors occurred when you applied filters to a group. (EMM-136820)
When you were using an LDAP connection, you couldn't synchronize user attributes. (EMM-136693)
SSAM requests failed when authentication didn't happen fast enough. (EMM-136097)
The Google APIs that BlackBerry Core uses were updated. (EMM-135730)
The Audit and Logging > System Audit page loads faster. (EMM-135518)
When an iOS device went out of compliance, the Root MDM Verification certificate was removed from the device. After the devices returned to an "in compliance" state, the Root MDM Verification certificate did not display on the device, and BlackBerry Dynamics apps remained in an application blocked state. (EMM-133296)
When a SSAM request arrived to a domain that contained multiple BlackBerry UEM instances, if most of the instances were not running, the response to the request was slow. (EMM-132636)

Fixed issues in BlackBerry UEM 12.11.1 quick fix 1

The unlock and clear password command did not work on iOS 13 devices. (EMM-133649)

Fixed issues in BlackBerry UEM 12.11.1

Installation, upgrade, and migration fixed issues

For migrations from on-premises BlackBerry UEM to on-premises BlackBerry UEM, UEM version 12.11 did not block the migration of BlackBerry Dynamics apps that were activated with the BlackBerry UEM Client. (EMM-127771)
Devices that were already pending migration might have displayed as device migration candidates. (EMM-127345)

User and device management fixed issues

When 2 iOS devices were activated for the same user, optional VPP apps could not be installed on both devices. (EMM-127393)
When you activated an Android device, Google Play might not have opened automatically and installed required apps. (EMM-124880)

Management console fixed issues

When you configured a connection between BlackBerry UEM and Microsoft Intune, and created a Microsoft Intune app protection profile, a corresponding profile was created on the Intune portal. If you later deleted the profile in the BlackBerry UEM console, the profile might not have been deleted from the Intune portal. (EMM-127748)
When you set the 'Required security patch level is not installed' option in a compliance profile, if BlackBerry UEM detected that a device had the incorrect patch level, the following incorrect message might have displayed: "Required security patch level was not detected by BlackBerry Dynamics, hardware attestation failed, or no BlackBerry Dynamics apps provided attestation results within the specified grace period: No action will be applied." (EMM-127708)
When you created a custom administrator role, if you chose the 'Selected groups only' option, and assigned the role to a user, that administrator user could not delete user groups from other users. (EMM-126379)
On the Apps page, if you filtered by "Apps needing review," warning icons might not have displayed beside some of the apps that needed review. (EMM-125724)

UEM Self-Service fixed issues

Certificate-based authentication did not work in UEM Self-Service when a user accessed UEM Self-Service using the BlackBerry UEM FQDN. (EMM-125721)

Known issues in BlackBerry UEM 12.11 MR1

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

Installation, upgrade, and migration known issues

* 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.

If you have applied an IT policy pack on your organization's BlackBerry UEM 12.10 MR1 server and you upgrade to BlackBerry UEM 12.11, the new IT policies are not hidden even though the policy pack was installed on the BlackBerry UEM 12.10 MR1 server. (EMM-129252)

Workaround: The policies will be hidden during the next policy sync or you can re-apply the IT policy pack manually.

You can't upgrade from UEM 12.9 to UEM 12.11 if the directory path contains brackets. For example, C:\Program Files (EXAMPLE)\BlackBerry\UEM\. (EMM-126340)

When you are migrating apps from Good Control to BlackBerry UEM, if you have not configured a policy that contains an authentication delegate in Good Control but BlackBerry UEM has a policy that configures app A as an authentication delegate, when you migrate app B, the app is blocked from migrating because app A has not been migrated. If you then migrate app A, app B will still be blocked because it does not send a request to app A to see if it has been migrated. (GD-31948)

Workaround: On the device, force the apps to stop and then restart app B.

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.

* You can't modify and save an enterprise connectivity profile that has iOS VPN on demand rules configured. (EMM-132378)

Workaround: Do not configure VPN on demand rules for iOS devices in an enterprise connectivity profile.

* If you modify an existing app lock mode profile for a Samsung Knox devices, the updated profile is not correctly updated on the device. (EMM-131626)

Workaround: Create a new app lock mode profile and assign it to the device.

iOS DEP devices can't authenticate with BlackBerry UEM during activation if the password contains special characters such as £. (EMM-126396)

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)
If your organization is using Entrust smart credentials on iOS, if you deactivate a device, the certificates still display as being imported on the Profiles screen. (EMA-10401)
After an iOS user imports a certificate, the user is taken through the import process again. (G3IOS-18108)
When you use a Work space only activation type to activate an Android 8.0 device and you configure a Wi-Fi profile in BlackBerry UEM, the device user might not be able to connect to a Wi-Fi network. (EMA-9175) **Workaround**: In your organization's IT policy, select the “Allow changing Wi-Fi settings" option. Note that this issue is fixed in Android 8.1.
When you use a Samsung Knox activation profile to activate an Android device and you select the "Google Play app management for Samsung Knox Workspace devices" option, the device will not activate and a Google Play services error will display. For more information, visit support.blackberry.com/community to read article KB46917. (EMA-9091)
On a Samsung Knox device, required BlackBerry UEM hosted apps might not display in the "Installed" section when the user opens Google Play on the device, even if they are actually installed. (EMM-95231)
You can't re-activate a macOS device if you remove the activation profile on the device. (EMM-92167)

Management console known issues

In a BlackBerry UEM and BES5 integrated environment, if you delete a BlackBerry OS user from the BlackBerry Administration Service without selecting the "Delete the user and remove the BlackBerry information from the user’s mail system" option, and then you add the same user to BlackBerry UEM and activate a BlackBerry OS device for the user, the BlackBerry OS device information does not display in the BlackBerry UEM management console.
* Attempting to upload an APK file for an internal app fails when using AdoptOpenJDK. (EMM-130584) **Workaround:** Use OracleJDK instead.
* In the Apps section of the BlackBerry UEM management console, if you select an app category and then perform a search on the filtered results, after the search the app categories no longer display. (EMM-130581) **Workaround:** Sign out and then back into BlackBerry UEM.

* 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.

When a DEP connection fails because a new token is generated on the Apple DEP portal, you don't receive an event notification email message. (EMM-126723)

You can save an iOS app shortcut that has a space in the URL. (EMM-126319)

When you click Managed devices or All users, select a user, resize the window, and click the back arrow, the screen that displays is empty. (EMM-125716)

Workaround: Click Managed devices or All users again.

A warning message does not display when you create an activation profile for an Android device and you do not select an activation type. (EMM-123636)

Workaround: Select an activation type.

If you schedule a directory synchronization job for offboarding Microsoft Active Directory users, the synchronization job might fail.(EMM-116146)

Workaround: Manually perform the directory synchronization job.

If you change the settings of a SCEP profile or user credential profile based on a native keystore, users are not prompted to enroll the certificates again and only new certificates receive the updated settings. (GD-37857)

Workaround: Delete the profile and create and assign a new one to apply the new settings.

In the BlackBerry Dynamics profile, if you upload a list that has more than 10000 banned passwords, it is truncated at 10000 passwords. (EMM-101809)

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)

When you create an IT policy for Android devices, the "Force the device and work space passwords to be different" rule implies that the personal and work space passwords must be different. However the passwords can be the same, although they are separate. (EMM-91416)

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

When you delete a user that is enable to use BlackBerry Workspaces, the message that displays is misleading. (EMM-78607)

Workaround: Log in to the console as a BlackBerry Workspaces Organization administrator who has an email address, remove the BlackBerry Workspaces service from the user, and then delete the user.

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)

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