



# **BlackBerry UEM Cloud**

## **Release Notes**



# Contents

What's new in BlackBerry UEM Cloud.....4

Fixed issues..... 9

Known issues..... 10

Legal notice..... 12

# What's new in BlackBerry UEM Cloud

## Migration

- **Migration of Android Enterprise devices:** Customers who have configured BlackBerry UEM to manage Google Play accounts can now migrate Android Enterprise devices from an on-premises BlackBerry UEM server to BlackBerry UEM Cloud or another on-premises BlackBerry UEM server. The on-premises BlackBerry UEM server must be version 12.13 or later.
- **Migration of BlackBerry Dynamics users:** You can now migrate BlackBerry Dynamics users from on-premises BlackBerry UEM (version 12.13 or later) to BlackBerry UEM Cloud.

## Management console

- **App protection profiles update:** Microsoft Intune app protection profiles have added support for recent Microsoft Intune feature updates.
- **Specify browser:** You can now specify which browser opens web links in apps managed by Microsoft Intune.
- **Factory reset protection profile improvements:** For factory reset protection profiles, you no longer need to manually obtain the User ID when you specify Google accounts that can unlock a device that has been reset to factory settings.
- **Delete users for value-added services:** You can now delete users who have additional value-added services assigned unless the user can't be removed from the service.
- **Event notifications:** The following event notifications were added:
  - Connectivity > Service connections for UEM instance changed: This notification alerts you when the connection status changes for the BlackBerry Affinity Manager, BlackBerry Secure Gateway, BlackBerry Proxy, or BlackBerry Secure Connect Plus service.
  - Server certificates > Certificate expiry: This notification alerts you when a server certificate is about to expire.

## BlackBerry Dynamics

- **BlackBerry Dynamics screen capture detection on iOS devices:** You can enable an option in a compliance profile that reacts to screen captures of BlackBerry Dynamics apps on iOS devices. When you enable this option, you can specify the allowed number of screen captures per time period, how long a period lasts, an enforcement action to occur if the user exceeds the allowed number of screen captures, and how long the enforcement action lasts. The allowed number of screen captures is per app. If the user exceeds the number of screen captures on one app, they are prevented only from using that app, not all BlackBerry Dynamics apps.

If you enable the option and set the enforcement action to "Monitor and log", when a user takes a screen capture, a warning message stating screen captures are prohibited is displayed on the device. If you enable the option and you set the enforcement action to "Do not allow BlackBerry Dynamics apps to run", when the user exceeds the number of screen captures, a message that informs the user how long they are prevented from taking screen captures is displayed on the device, and the user is blocked from using the app for the period that you specified in the compliance profile. All violations are logged in a compliance violation report for BlackBerry Dynamics apps.

- **Improvements to the BlackBerry Dynamics app activation process:** Administrators and users can now activate BlackBerry Dynamics apps using simple passwords (for example, a password of any length) or QR codes in addition to the 15-character access key. This simplifies the activation process for users. Activating BlackBerry Dynamics apps using a password or QR code is the preferred method of activating apps. This feature requires that apps use BlackBerry Dynamics SDK 8.0 or later.

- **Improvements to unlocking BlackBerry Dynamics apps:** Administrators can now send a QR code to a user to unlock a BlackBerry Dynamics app. Users with access to BlackBerry UEM Self-Service can use the QR code to unlock the app instead of the unlock key. This feature requires that apps use BlackBerry Dynamics SDK 8.0 or later.

## Apple

- **Automatic activation of a BlackBerry Dynamics app for Apple DEP and User Enrollment devices:** For Apple DEP devices and devices that are activated with Apple User Enrollment, a BlackBerry Dynamics app can be preconfigured so that it automatically activates during device enrollment without requiring the user to manually enter information. If the app is an authentication delegate, it can be used to easily activate other BlackBerry Dynamics apps.
- **iOS New Capabilities:** For iOS devices with eSIM cellular plans, administrators can request updated plan information from the carrier.

## Chrome OS

- **Management of Chrome OS devices:** You can now manage Chrome OS devices separately from Android devices in the following ways:
  - On the Dashboard, in Devices by platform, Chrome OS devices are shown.
  - In Users > Managed devices, Chrome is now an option for the OS filter.
  - In Groups > Device, you can create device groups based on Chrome OS.
  - In Migration > Migrate devices, Chrome OS devices are shown

## Windows 10 devices

- **Support for Windows Hello for Business:** For Windows 10 devices, you can now choose whether to allow biometric gestures (such as facial or fingerprint recognition) in the IT policy. You can also enable enhanced anti-spoofing for when facial recognition is configured on the device. These settings require Windows 10 version 1511 or later.

## BEMS Cloud

- **Trusted connection between BEMS-Docs and Microsoft SharePoint:** You can now import and remove individual CA and Intermediate certificates from the BEMS Cloud database using the BlackBerry UEM console. This allows administrators to import and replace individual self-signed and custom CA certificates to create the trusted connection between BEMS-Docs and Microsoft SharePoint.
- **BEMS Cloud repository enhancements:** You can now use the new users tab in the BEMS Cloud Docs service to search for users, view administrator defined repositories that users have access to, and view repositories that authorized users created. For administrator defined repositories, administrators can override the path and view the access permissions that users have.
- **Updated repository error messages:** When a repository is not successfully defined, a custom error message displays that explains why the repository did not save properly (for example, if you create a repository using the same name as one that exists, the error message Repository already exists with name <repository name> displays). This allows the user and IT personnel to diagnose and fix the problem.

## Documentation

- The [BlackBerry Docs site](#) has improved search and navigation tools to make it easier to find docs for products and features. Click the magnifying glass in the top navigation bar to perform a keyword search. You can filter results by product, version, and document type.

You can also click [Let us help you find something](#) on the home page and [BlackBerry UEM](#) page to open a Doc Map that will point you to the right doc, whether you're looking for product information to help make a purchase decision or you're already a customer and need administrator, end-user, or developer help.

- A beta version of an easy-to-use online version of the Performance Calculator will be available soon. You will be able to access it on the [BlackBerry UEM Planning and architecture documentation](#) web page.

## New IT policy rules

Device type	Name	Description	Activation types
Windows	Allow use of biometric gestures	Enable or disable the use of biometric gestures, such as face and fingerprint, as an alternative to the PIN gesture for Windows Hello for Business.	MDM controls
Windows	Enable enhanced anti-spoofing for facial feature recognition	Enable or disable enhanced anti-spoofing for facial feature recognition on Windows Hello face authentication.	MDM controls
Android Global (all Android devices)	Obtain time zone from network	Specify whether the device obtains the time zone from the network.	Work space only, Work and personal - full control
Android Global (all Android devices)	Device time zone	Specify the time zone that the device uses. For a list of possible values, see the IT Policy Reference.	Work space only, Work and personal - full control
Android Global (all Android devices)	Allow ambient display	Specify whether the user can enable ambient display on the device. Ambient display shows notifications on the lock screen when the device is locked.	Work space only, Work and personal - full control
Android Global (all Android devices)	Allow airplane mode	Specify whether the user can enable airplane mode on the device.	Work space only, Work and personal - full control

Device type	Name	Description	Activation types
Android Work profile (all Android devices)	Force the device and work profile passwords to be different	Specify whether the device and work profile passwords must be different when a work profile password is required by the Android work profiles "Password requirements" rule.	Work and personal - user privacy, Work and personal - full control
Android Work profile (all Android devices)	Allow printing	Specify whether the user can print files using the device OS print functionality. This rule does not block sharing files to apps that can send files to a printer.	Work space only, Work and personal - user privacy, Work and personal - full control
Android Work profile (all Android devices)	Allow user to configure location	Specify whether the user can turn the location feature on or off.	Work space only, Work and personal - user privacy, Work and personal - full control
Android Work profile (all Android devices)	Allow personal data in work profile	Specify whether files and data in the personal profile can be sent to the work profile or accessed from work apps.	Work and personal - user privacy, Work and personal - full control
Android Work profile (all Android devices)	Allow biometrics	Specify whether the user can use biometric authentication to unlock the device.	Work space only, Work and personal - user privacy, Work and personal - full control
Android Work profile (all Android devices)	Allow facial recognition	Specify whether the user can unlock the device using face recognition.	Work space only, Work and personal - user privacy, Work and personal - full control
Android Work profile (all Android devices)	Allow iris authentication	Specify whether the user can unlock the device using an iris scan.	Work space only, Work and personal - user privacy, Work and personal - full control

Device type	Name	Description	Activation types
Android Work profile (all Android devices)	Apps restricted from metered networks	Specify the apps that are restricted from using metered data networks. You may want to restrict app network usage due to data costs and limits or battery and performance issues.	Work space only, Work and personal - user privacy, Work and personal - full control
Android Personal profile (all Android devices)	Allow biometrics	Specify whether the user can use biometric authentication to unlock the device.	Work and personal - full control
Android Personal profile (all Android devices)	Allow facial recognition	Specify whether the user can unlock the device using face recognition.	Work and personal - full control
Android Personal profile (all Android devices)	Allow iris authentication	Specify whether the user can unlock the device using an iris scan.	Work and personal - full control
Android Personal profile (all Android devices)	Allow printing	Specify whether the user can print files using the device OS print functionality. This rule does not block sharing files to apps that can send files to a printer.	Work and personal - full control



# Fixed issues

## Management console fixed issues

After you upgraded BlackBerry UEM, a user with the Junior HelpDesk role could not set an activation password. (EMM-142625)

When you tried to use the "Change password and lock device" command in the management console for a device that was activated using an Android Enterprise activation type, if you had configured the IT policy to use 'Numeric Complex' passwords, an error displayed that stated the password did not meet the minimum requirements. (EMM-141537)

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

After you provisioned BlackBerry Intelligent Security, you could not use the BlackBerry UEM management console. (EMM-141419)

You might not have been able to remove a VPP account that had many users. (EMM-141084)

If an administrator did not have the "View User Credential Profile" permission assigned and you created a user credential profile to manually upload certificates, the administrator could not upload or replace certificates. (EMM-141001)

The "Tenant attestation enabled date" was updated in the database when you clicked Save on the Attestation page. (EMM-140416)

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

On the device tab, if you tried to upgrade the software version on a supervised iOS device to a specific version number, when you clicked on Download and install, the OS was downloaded but not installed. (EMM-135440)

## BlackBerry Secure Connect Plus fixed issues

After you upgraded to BlackBerry UEM 12.12, the BlackBerry Secure Connect Plus service might not have started and stayed running if syslog was configured for localhost. (EMM-139980)

# Known issues

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

## Migration known issues

\* During migration, after you refresh the "Migrate users" page, sometimes no records are displayed. (EMM-143257)

## 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.

\* On an Android Enterprise device, users can turn the location feature on even if the setting is turned off by the IT policy. (EMM-143162)

The BlackBerry UEM Core does not send the Device IMEI value to the Lookout for Work app when the app activates. (EMM-140895)

If a junior help desk administrator does not have the "View factory reset protection profiles" permission enabled, an error occurs when the junior help desk administrator clicks on a user. (EID-12919)

**Workaround:** Assign the "View factory reset protection profiles" permission to the administrator.

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

\* When you offboard synchronized users, if any of the users is enabled to use BBM Enterprise, the user is deactivated but still displays in the console. (EMM-143941)

**Workaround:** Resynchronize the users.

\* If you try to export users to a .csv file from the "Managed devices" screen, when you open the file, none of the users' information is displayed. (EMM-142661)

\* When you try to update the category information for the Zoom app, an error displays. (EMM-143641)

\* You can't delete user accounts that have an activated BlackBerry Dynamics app assigned to them. (EMM-143623)

\* When you click "Add" in the "App servers" section of a BlackBerry Dynamics Connectivity profile, any apps that have multiple binaries are duplicated on the "Select a BlackBerry Dynamics app" page. (EMM-143152)

\* If you use custom self-service activation messages and the custom message contains %ActivationQRCode % as part of the message, users can't set their own activation passwords in BlackBerry UEM Self-Service. (EMM-142869)

\* After you add a user to multiple user groups, only the "all users" group displays in the 'Member of groups' list on the 'Add to user groups' page. (EMM-142751)

If you use a REST call to create a compliance policy and you set the iOS hardware restriction to false, the error message that displays does not provide the administrator with enough information to successfully create the profile. (EMM-140868)

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.

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 *myAccount* 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

# Legal notice

©2020 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada