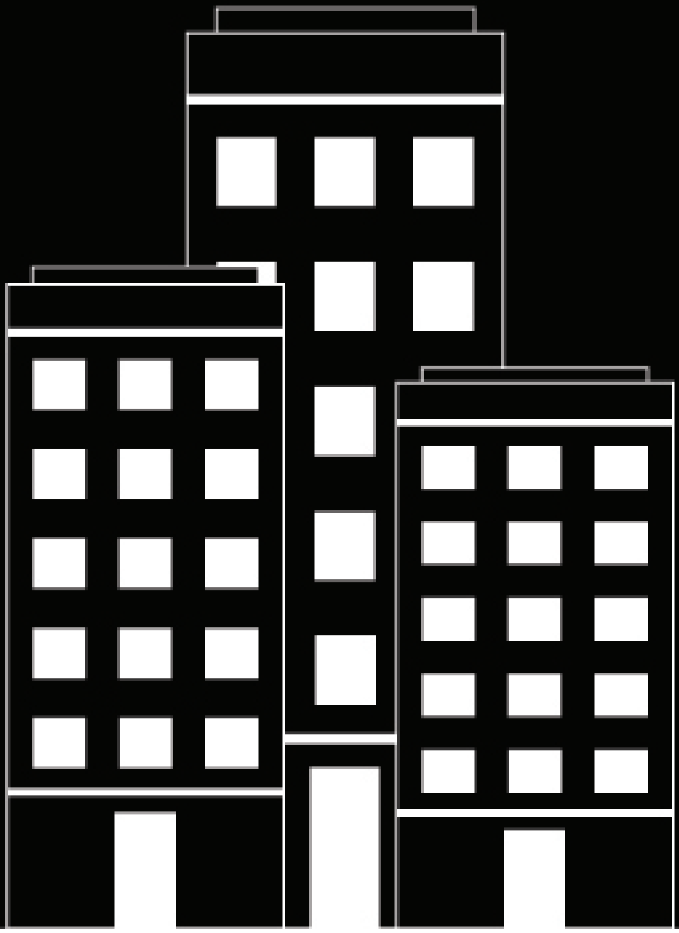

BlackBerry UEM

Overview and What's New

12.10 Maintenance release 1

Contents

What's new in BlackBerry UEM 12.10 MR1

- **Installation/Third-Party Software**: OpenJDK 8-based builds that are compatible with Java SE 8 are now supported as an alternative to using Oracle JDK 8. These builds and support are available from vendors such as Azul Systems (Zulu) or AdoptOpenJDK. For information about supported JRE versions, see the BlackBerry UEM Compatibility Matrix, KB54036, and KB52117.
- **Factory reset protection for Android Enterprise devices**: You can set up a Factory reset protection profile for your organization's Android Enterprise devices that have been activated using the Work space only activation type. This profile allows you to specify a user account that can be used to unlock a device after it has been reset to factory settings, or remove the need to sign in after the device has been reset to factory settings.
- **Update period for apps that are running in the foreground**: On devices that are activated with Android Enterprise, you can set an update period for apps that are running in the foreground because by default, when an Android app is running in the foreground, Google Play cannot update it. You can also control how Google Play applies the changes to the device such as the user can allow the change, or the change occurs only when the device is connected to a Wi-Fi network.
- **Fingerprint authentication**: You can now open the BlackBerry UEM Client and configure fingerprint authentication after BlackBerry Dynamics app activation is complete.
- **TLS 1.2**: All SSL connections between BlackBerry UEM and BlackBerry UEM Cloud and other internal and external systems now use TLS 1.2.
- **Support for deploying B2B apps licensed with your Apple VPP account:** If you have obtained B2B apps using your Apple VPP account and added your VPP account to BlackBerry UEM, you can now assign those apps to users and groups in BlackBerry UEM.

New IT policy rules

Device type	Name	Description
iOS	Allow the user to remove or add a cellular plan to the eSIM on the device (supervised only)	Specify whether the user is able to remove or add a cellular plan to the eSIM on the device.
iOS	Allow changing cellular plan settings (supervised only)	Specify whether the user can change settings related to their cellular plan.

What's new in BlackBerry UEM 12.10

Android

Enable Android Enterprise for all Android Enterprise instances: The configuration wizard that appears on initial log in to BlackBerry UEM now allows administrators to configure Android Enterprise. (JI 2539585)

Android SafetyNet improvements: The following improvements were made for Android SafetyNet support:

- A Google SafetyNet attestation failure option was added to the compliance profile. This option creates a compliance rule that specifies the actions that occur if devices do not pass SafetyNet attestation.
- An app grace period was added to the Android SafetyNet configuration.
- You can add a list of BlackBerry Dynamics apps that receive attestation challenges.

Policies for Android Enterprise devices: Policies have been added for logging of SMS, MMS and phone calls on Android Enterprise devices. You can enable the logging in a server group or in the default settings of the BlackBerry Connectivity Node setup page. You must upgrade the BlackBerry Connectivity Node to the most recent version before you can use this feature. (JI 856189)

Specify which certificates are used with Android apps: A new certificate mapping profile allows you the specify which user credential, SCEP, or shared certificate profile is used when an Android app requires a certificate. (JI 2517869)

Android app-based PKI: You can now use an app-based PKI solution such as Purebred with BlackBerry Dynamics apps on Android devices. (JI 1965015)

Samsung KNOX support: BlackBerry UEM now supports devices running Samsung KNOX 3.2. (JI 2573555)

Support for Samsung KNOX policies on Android Enterprise for all BlackBerry UEM activations: The benefits of Samsung KNOX are now available to Samsung KNOX devices when the devices are activated with an Android Enterprise activation type. Samsung KNOX devices that are activated with an Android Enterprise activation type now have Samsung KNOX policies applied. Even though devices already activated with a Samsung KNOX activation type continue to work, the Android Enterprise activation types are recommended for new activations. (JI 2510232)

Samsung KNOX activation type	Recommended Android Enterprise activation type
Work and personal - full control (Samsung KNOX)	Not applicable. Continue to use the Work and personal - full control (Samsung KNOX) activation type.
Work and personal - user privacy - (Samsung KNOX)	Work and personal - user privacy - (Android Enterprise): No KNOX policies are applied to the device. If you want to apply KNOX policies in the work space, select “When activating Android Enterprise) devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus”

Work space only - (Samsung KNOX)	Work space only (Android Enterprise): KNOX MDM policies are applied to the device. If you want to apply KNOX policies in the work space, select “When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus.”

iOS

Event notification: A new Administration section was added to the Event notifications page. The section contains a field that allows you to set up a notification that is sent when an administrator account gets locked. (JI 2529062)

Device unenrollment notification: The event notification that you receive for device unenrollment now includes the reason that the unenrollment occurred. (JI 2565941)

New S/MIME settings: New settings are available for iOS 12 and later devices. (JI 2571842)

iOS: email profile settings	Description
User can toggle S/MIME signing	This setting specifies whether a user is allowed to turn the signing setting on/off. This setting applies only to iOS 12.0 and later devices
User can change signing credentials	This setting specifies whether a user is allowed to change signing credentials. This setting applies only to iOS 12.0 and later devices.
User can override S/MIME encryption	This setting specifies whether a user is allowed to turn the encryption setting on/off. This setting applies only to iOS 12.0 and later devices.
User can override S/MIME encryption credentials	This setting specifies whether a user is allowed to change S/MIME encryption credentials. This setting applies only to iOS 12.0 and later devices.

Per-app notification: When you are configuring per-app notifications for an iOS device, you can select the following new options:

- Enable critical alert: This option specifies whether a critical alert can override the do not disturb profile and notification settings. This setting applies only to iOS 12.0 and later devices.
- Show in CarPlay: This option specifies whether notifications display in Apple CarPlay. This setting applies only to iOS 12.0 and later devices.

Work app catalog search: Users can now perform a search in the work app catalog to easily find apps that are assigned to them.

BlackBerry Dynamics

App deployment reports: For BlackBerry Dynamics apps, you can export app deployment reports to an .html file from the Apps screen in the management console. The report includes information about apps deployed by BlackBerry UEM and the users that have installed the apps on their devices. The report now includes a Status column that provides a status of the apps on each device, such as installed and not installed. (JI 2565954)

BlackBerry Dynamics access key email: When you generate BlackBerry Dynamics access keys for a user, you can specify whether to send an activation email to the user. (JI 2578997)

SCEP improvement: You can now configure BlackBerry Dynamics apps to use SCEP to retrieve certificates. (JI 2532872)

Installation

Remove BlackBerry Collaboration Service, JRE, and JCE deployment from setup.exe: As of BlackBerry UEM release 12.10, the BlackBerry Collaboration Service and JRE are no longer bundled with the installer. If you are installing BlackBerry UEM, you must first download and install JRE (minimum version JRE 8u151).

Certificates

Certificate-based authentication improvement: BlackBerry UEM now supports certificate-based authentication for logging in to the management console and UEM Self-Service. (JI 1465040)

BlackBerry UEM Notifications

User synchronization service from UEM: UEM administrators can now ensure all of their users are in the BlackBerry AtHoc system by synchronizing users from within the UEM console. Administrators can set up a user synchronization service as a system job that updates users periodically and keeps track of the changes.

New IT policy rules

Device type	Group	Name	Description
Android	Global (all Android devices)	Allow outgoing calls	Specify if a user can place outgoing calls. If this rule is not selected, the device can only make emergency calls. All other outgoing calls are blocked.
Android	Global (all Android devices)	Send SMS/ MMS logs to the BlackBerry Connectivity Node	Specify whether the device synchronizes logs for SMS text messages and MMS messages with your EMM server.
Android	Global (all Android devices)	Send phone logs to the BlackBerry Connectivity Node	Specify whether the device synchronizes the call log for the Phone app with your EMM server.
Android	Global (Samsung KNOX devices only)	Allow NFC	Specify whether a device can use NFC.
Android	Global (Samsung KNOX devices only)	Allow OTA updates	Specify if a device can update its OS using a Firmware Over-The-Air (FOTA) client (for example, Samsung KNOX EMM or WebSync DM). If this rule is not selected, all wireless update requests (user-initiated, server-initiated, and system-initiated) are blocked. The user may see messages related to new OS updates but any attempt to update the OS fails.

Device type	Group	Name	Description
Android	Global (Samsung KNOX devices only)	Allow Wi-Fi	Specify whether a device can make Wi-Fi connections. After you deselect this rule and then reselect it, the device cannot use Wi-Fi until it is restarted.
Android	Global (Samsung KNOX devices only)	Allow Wi-Fi Direct	Specify if a device can use Wi-Fi Direct. When this rule is selected, the device can make connections using Wi-Fi Direct. This rule also affects the S Beam feature on Samsung devices.
Android	Global (Samsung KNOX devices only)	Allow tethering	Specify if a device can share its mobile network connection with other devices using Bluetooth. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow Bluetooth tethering	Specify if a device can share its mobile network connection with other devices using Bluetooth. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow USB tethering	Specify if a device can share its mobile network connection with other devices using USB. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow Wi-Fi tethering	Specify if a device can share its mobile network connection with other devices using Wi-Fi. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow firmware recovery	Specify if a user can update the operating system of a device using download mode.
Android	Global (Samsung KNOX devices only)	Require SD card encryption	Specify if a device must encrypt all data on the external SD card. This rule requires the value of the "Password requirements" rule to be at least "Alphanumeric."

Device type	Group	Name	Description
Android	Work profile (Samsung KNOX devices only)	Require certificate revocation (CRL) check for apps	Specify if apps must check for revoked certificates in the server certificate chain when opening SSL connections in KNOX Workspace. This rule applies only to apps that use the standard Java SSL sockets and TrustManager implementation (including most native apps), but does not apply to third-party browsers. The certificate revocation check uses CRLs from the CRL distribution point listed in the certificates. If the "Require OCSP check" rule is selected, apps first check for certificate revocation using OCSP. If OCSP fails, then apps check the CRLs.
Android	Work profile (Samsung KNOX devices only)	Require OCSP check for apps	Specify if apps must use OCSP before using CRLs to check for revoked certificates when opening SSL connections in KNOX Workspace. The OCSP check uses the OCSP response server in the "Authority Information Access" extension in the certificate.
Android	Work profile (Samsung KNOX devices only)	Validate end-user installed certificates	Specify whether the device validates certificates installed by end users. If one of the validation checks (for example, certification path, expiration date, or revocation status) fails, the device blocks the installation of the certificate.
Android	Work profile (Samsung KNOX devices only)	Allow "Share via" list	Specify whether a work app can display the "Share via" list to allow a user to share content across work apps in the Workspace.
Android	Work 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 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 Workspace only.

Device type	Group	Name	Description
Android	Work 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.
Android	Work profile (Samsung KNOX devices only)	Allow video recording	Specify if a device can record video. If this rule is not selected, the camera is still available so that a user can take pictures and use video streaming. If you deselect this rule, any ongoing video recording is interrupted.
Android	Work profile (Samsung KNOX devices only)	Enable JavaScript	Specify whether the native Android browser prevents the browser from running JavaScript code for a website. If this rule is not selected, a website that requires JavaScript to be active to execute a function (for example, an animation) cannot execute the function. If this rule is not selected, a user cannot change the setting on the device.
Android	Work profile (Samsung KNOX devices only)	Allow fingerprint authentication	Specify whether the user can use fingerprint authentication for the KNOX Workspace.
Android	Work profile (Samsung KNOX devices only)	Allow iris authentication	Specify whether a user can authenticate with the work space using an iris scan.
Android	Work profile (Samsung KNOX devices only)	Allow password visibility	Specify whether the Workspace password is visible when a user is typing it. If this rule is not selected, users and apps cannot change the visibility setting.
iOS	Security and privacy	Allow managed apps to add contacts to unmanaged accounts	Specify whether users can add contacts from managed apps to unmanaged contacts accounts.
iOS	Security and privacy	Allow unmanaged apps to read contacts from managed accounts (supervised only)	Specify whether unmanaged apps can read contacts from managed contacts accounts.

Device type	Group	Name	Description
Windows Phone	Security and privacy	Default app access to diagnostic information	Specify whether apps can access device diagnostic information about other apps by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access diagnostic information. If you select "Disallow," apps can't access diagnostic information.
Windows Phone	Security and privacy	Apps allowed access to diagnostic information	Specify the list of apps that are always allowed to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule.
Windows Phone	Security and privacy	Apps not allowed access to diagnostic information	Specify the list of apps that are never allowed to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule.
Windows Phone	Security and privacy	App access to diagnostic information controlled by user	Specify the list of apps that users can choose to allow to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule.
Windows Phone	Security and privacy	Default apps can run in background	Specify whether apps can run in background by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can run in background. If you select "Disallow," apps can't run in background.
Windows Phone	Security and privacy	Apps allowed to run in background	Specify the list of apps that are always allowed to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule.

Device type	Group	Name	Description
Windows Phone	Security and privacy	Apps not allowed to run in background	Specify the list of apps that are never allowed to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule.
Windows Phone	Security and privacy	App ability to run in background controlled by user	Specify the list of apps that users can choose to allow to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule.

What is BlackBerry UEM?

BlackBerry UEM is a multiplatform EMM solution from BlackBerry that provides comprehensive device, application, and content management with integrated security and connectivity, and helps you manage iOS, macOS, Android, Windows 10, BlackBerry 10, and BlackBerry OS (version 5.0 to 7.1) devices for your organization.

BlackBerry UEM offers trusted end-to-end security and provides the control that organizations need to manage all endpoints and ownership models. For information about trying BlackBerry UEM, see the information on blackberry.com.

Feature	Benefit
Low total cost of ownership	BlackBerry UEM reduces complexity, optimizes pooled resources, ensures maximum uptime and helps you achieve the lowest total cost of ownership.
Single web-based interface	Manage iOS, macOS, Android, Windows 10, and BlackBerry 10 devices all from a single management console.
Flexible ownership models	Use a set of customizable policies and profiles to manage BYOD, COPE, and COBO devices, and protect business information.
User and device reporting	Manage fleets of devices using comprehensive reporting and dashboards, dynamic filters, and search capabilities.
Simple user set up and enrollment	Allow users to activate their own devices with BlackBerry UEM Self-Service.
Industry-leading mobile security	BlackBerry UEM leverages the BlackBerry Infrastructure to ensure data security across iOS, macOS, Android, Windows, and BlackBerry devices.
High availability	Configure high availability to minimize service interruptions for device users.
Additional services available	Enable services such as BlackBerry Workspaces, BlackBerry 2FA, and BlackBerry UEM Notifications that allow you to add value to your BlackBerry UEM deployment.

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

BlackBerry Enterprise Mobility Suite services

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

Service type	Service name and description
Enterprise services	• BlackBerry Workspaces allows users to securely access, synchronize, edit, and share files and folders from Windows and Mac OS tablets and computers or Android, iOS, and BlackBerry 10 devices. BlackBerry Workspaces protects files by applying DRM controls to limit access, even after they are shared with someone outside of your organization. • BlackBerry Enterprise Identity gives users single sign-on access to service providers such as BlackBerry Workspaces, Box, Workday, WebEx, Salesforce, and more. You can also add support for custom SaaS services. • BlackBerry 2FA protects access to your organization's critical resources using two-factor authentication. BlackBerry 2FA uses a password that users enter and a secure prompt on their Android, iOS, or BlackBerry 10 devices each time they attempt to access resources. • BlackBerry UEM Notifications allows administrators to message users via SMS, phone, and email directly from the UEM console. This add-on simplifies communications to end users and user groups, by eliminating the need for additional messaging solutions.
BlackBerry Dynamics platform	• The BlackBerry Enterprise Mobility Server (BEMS) provides additional services for BlackBerry Dynamics apps. BEMS integrates the following services: BlackBerry Mail, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs. When these services are integrated, users can communicate with each other using secure instant messaging, view the real-time presence of users in BlackBerry Dynamics apps, and access, synchronize, and share work file server and Microsoft SharePoint documents. • The BlackBerry Dynamics SDK allows developers to create secure apps for Android and iOS devices and Mac OS and Windows computers. It is the client side of the BlackBerry Dynamics platform.
BlackBerry Dynamics productivity apps	• BlackBerry Work provides everything users need to securely mobilize their work, including email, calendar, and contacts (full synchronization with Microsoft Exchange). The app also provides advanced document collaboration. BlackBerry Work separates work data from personal data and allows seamless integration with other work apps without requiring MDM profiles on the device. • BlackBerry Access enables users to securely access their organization's intranet with their mobile device of choice. • BlackBerry Connect enhances communication and collaboration with secure instant messaging, corporate directory lookup, and user presence, all from an easy-to-use interface on the user's device. • BlackBerry Tasks allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their Android and iOS devices. • BlackBerry Notes allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their mobile device of choice.

For more information about the different BlackBerry Enterprise Mobility Suite licenses and how to obtain them, see the Licensing content.

Benefits of BlackBerry Workspaces

BlackBerry Workspaces is the leading secure Enterprise File Sync and Share (EFSS) solution. It allows users to access content anytime, anywhere, and file share inside and outside their organization. BlackBerry Workspaces embeds Digital Rights Management (DRM) protection into files, so content remains secure and within your control, even after it's downloaded and shared. With a secure file store and the ability to transfer data while maintaining control, both employees and IT can be confident in data sharing and document security.

For more information about the benefits of BlackBerry Workspaces, see the information on blackberry.com.

Benefits of BlackBerry Enterprise Identity

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

BlackBerry Enterprise Identity is offered in the BlackBerry Enterprise Mobility Suite - Application Edition and BlackBerry Enterprise Mobility Suite - Content Edition.

For more information about the benefits of BlackBerry Enterprise Identity, see the information on blackberry.com.

Benefits of BlackBerry 2FA

BlackBerry 2FA provides two-factor user authentication through a password and a user's device, and leverages your existing iOS, Android, or BlackBerry devices to deliver a simple user experience that protects your organization's security.

BlackBerry 2FA is offered in the BlackBerry Enterprise Mobility Suite - Application Edition and BlackBerry Enterprise Mobility Suite - Content Edition.

For more information about the benefits of BlackBerry 2FA, see the information on blackberry.com.

Benefits of BlackBerry UEM Notifications

BlackBerry UEM Notifications simplifies communications to end users and user groups. Administrators can send critical messages and notifications to users from the UEM management console.

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

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

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

Enterprise apps

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

Component	Description
BlackBerry UEM Client	The BlackBerry UEM Client allows BlackBerry UEM to manage iOSand Androiddevices. Users must install the BlackBerry UEM Client before activating an iOSor Android device for mobile device management with BlackBerry UEM. Users can download the latest version of the BlackBerry UEM Client from the App Store for iOS devices and from Google Play for Android devices. After users activate their devices, the BlackBerry UEM Client allows users to do the following: • Verify whether their devices are compliant with the organization's standards • View the profiles that have been assigned to their user accounts • View the IT policy rules that have been assigned to their user accounts • Access work apps • Create access keys for BlackBerry Dynamics apps • Preauthenticate with BlackBerry 2FA • Access a software OTP code • Deactivate their devices For more information about the BlackBerry UEM Client, see the BlackBerry UEM Administrator content and the BlackBerry UEM Client end user content.
BlackBerry Dynamics apps	BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect provide users with access to work data and productivity tools.
BBM Enterprise	BBM Enterprise adds a layer of end-to-end encryption for BBM messages sent between BBM Enterprise users in your organization and other BBM users inside or outside of your organization. BBM Enterprise is available for iOS, Android, BlackBerry 10, Windows, and macOS devices. BBM Enterprise uses a FIPS 140-2 validated cryptographic library. Your organization owns the encryption keys and no one else, not even BlackBerry, can access them. For most devices, you can use BlackBerry UEM to assign BBM Enterprise to users. After you enable users to use BBM Enterprise, users can download the BBM Enterprise app from the App Store, the Google Play store, or BlackBerry World. For more information about BBM Enterprise, see the BBM Enterprise content.
BlackBerry Enterprise BRIDGE	BlackBerry Enterprise BRIDGE is a Microsoft Intune app that is enabled for BlackBerry Dynamics. It allows you to securely view, edit, and save documents using Intune-managed Microsoft apps, such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel in BlackBerry Dynamics on iOS and Android devices. For more information about BlackBerry Enterprise BRIDGE, see the BlackBerry Enterprise BRIDGE content.

BlackBerry Dynamics apps

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

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

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

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

Enterprise SDKs

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

Component	Description
BlackBerry UEM Integration SDK	The BlackBerry UEM Integration SDK allows developers to create plug-ins that extend the functionality of BlackBerry UEM. Using the UEM Integration SDK (which includes the UEM Integration plug-in for Eclipse) and the UEM Integration APIs, you can create and deploy BlackBerry UEM plug-ins that allow for the tight integration of new features or services with an existing BlackBerry UEM installation. For more information about the BlackBerry UEM Integration SDK, see the BlackBerry UEM Integration SDK content.

Component	Description
BlackBerry Dynamics SDK	The BlackBerry Dynamics SDK provides a powerful set of tools to ISV and enterprise developers, allowing them to focus on building their apps rather than learning how to secure, deploy, and manage those apps. The BlackBerry Dynamics SDK can be used to develop native, hybrid, and web apps for iOS, macOS, Android, and Windows devices, with services such as the following: • Security services (e.g., secure communications and interapp data exchange APIs) • Mobile services (e.g., presence, email, push, directory lookup) • Platform services (e.g., single sign-on authentication, indentity and access management, app-level controls for admins) For more information about the BlackBerry Dynamics SDK, see the BlackBerry Dynamics SDK content.
BlackBerry Analytics SDK	The BlackBerry Analytics SDK allows BlackBerry Dynamics app developers to enable custom BlackBerry Dynamics apps for Android and iOS to automatically record events and send them to BlackBerry Analytics. All you need to do is integrate the BlackBerry Analytics library into your app; the SDK does the work of sending the events for you. For more information about the BlackBerry Analytics SDK, see the BlackBerry Analytics content.
Spark Communications Services SDK	The BlackBerry Spark Communications Services SDK provides a framework to develop real-time, end-to-end secure messaging capabilities in your own product or service. The Spark Communications Services security model ensures that only the sender and intended recipient can see each message sent, and that messages aren't modified in transit between the sender and recipient. The Spark Communications Services SDK also provides the framework for other forms of collaboration and communication, such as push notifications, secure voice and video calls, and file sharing. You can even extend and create new types of real-time services and use cases by defining your own custom application protocols and data types. For more information about the Spark Communications Services, see the Spark Communications Services SDK content.
BlackBerry Web Services	The BlackBerry Web Services are a collection of SOAP and REST web services that you can use to create applications to manage your organization's BlackBerry UEM domain, user accounts, and all supported devices. You can use the BlackBerry Web Services to automate many tasks that administrators typically perform using the management console. For example, you can create an application that automates the process of creating user accounts, adds users to multiple groups, and manages users' devices. For more information about the BlackBerry Web Services, see the BlackBerry Web Services for BlackBerry UEM content.

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

Key BlackBerry UEM features

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

Feature	Description
Powerful app management	BlackBerry UEM is a comprehensive app management platform for all devices. You can deploy apps from all major app stores, including App Store, Google Play, Windows Store, and BlackBerry World storefront.
Role-based administration	You can share administrative duties with multiple administrators who can access the administration consoles at the same time. You can use roles to define the actions that an administrator can perform and reduce security risks, distribute job responsibilities, and increase efficiency by limiting the options available to each administrator. You can use predefined roles or create your own custom roles.
Company directory integration	You can use local, built-in user authentication to access the management console and self-service console, or you can integrate with the Microsoft Active Directory or LDAP company directories that you use in your organization's environment (for example, IBM Domino Directory). BlackBerry UEM supports connections to multiple directories. You can have any combination of both Microsoft Active Directory and LDAP. You can also configure BlackBerry UEM to automatically synchronize the membership of a directory-linked group to its associated company directory groups when the scheduled synchronization occurs. When you configure the settings for directory-linked groups, you can select offboarding protection. Offboarding protection requires two consecutive synchronization cycles before device data or user accounts are deleted from BlackBerry UEM. This feature helps to prevent unexpected deletions that can occur because of latency in directory replication.
Cisco ISE integration	Cisco Identity Services Engine (ISE) is network administration software that gives an organization the ability to control whether devices can access the work network (for example, permitting or denying Wi-Fi or VPN connections). This release allows you to create a connection between Cisco ISE and BlackBerry UEM so that Cisco ISE can retrieve data about the devices that are activated on BlackBerry UEM. Cisco ISE checks device data to determine whether devices comply with your organization’s access policies.
Synchronizing with a Good Control server	After you install BlackBerry UEM version 12.7 in an environment that has an existing Good Control server, you must synchronize Good Control with BlackBerry UEM to enable BlackBerry UEM version 12.7 features.

Feature	Description
Regional deployment	You can set up regional connections for enterprise connectivity features by deploying one or more BlackBerry Connectivity Node instances in a dedicated region. This is known as a server group. Each BlackBerry Connectivity Node includes BlackBerry Secure Connect Plus, the BlackBerry Gatekeeping Service, the BlackBerry Secure Gateway, BlackBerry Proxy, and the BlackBerry Cloud Connector. You can associate enterprise connectivity and email profiles with a server group so that any users that are assigned those profiles use a specific regional connection to the BlackBerry Infrastructure when using BlackBerry Connectivity Node components. Deploying more than one BlackBerry Connectivity Node in a server group also allows for high availability and load balancing.
Wearable devices	You can activate and manage certain Android-based, head-worn wearable devices in BlackBerry UEM. For example, you can manage Vuzix M300 Smart Glasses. Smart glasses provide users with hands-free access to visual information such as notifications, step-by-step instructions, images, and video and allow users to issue voice commands, scan bar-codes and use GPS navigation. Examples of BlackBerry UEM management capabilities that are supported include: Device activation using QR code, IT policies, Wi-Fi and VPN profiles, app management and location services.
Microsoft Intune integration	For iOS and Android devices, if you want to protect data in Microsoft Office 365 apps using the MAM features of Microsoft Intune, you can use Intune to protect app data while using BlackBerry UEMto manage the devices. Intune provides security features that protect data within apps. For example, Intune can require that data within apps be encrypted and prevent copying and pasting, printing, and using the Save as command. You can connect UEM to Intune, allowing you to manage Intune app protection policies from within the UEM management console.

Key features for all device types

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

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

Feature	Description
Control how devices connect to your organization's resources	You can use an enterprise connectivity profile to control how apps on devices connect to your organization’s resources. When you enable enterprise connectivity, you avoid opening multiple ports in your organization's firewall to the Internet for device management and third-party applications such as the mail server, certification authority, and other web servers or content servers. Enterprise connectivity sends all traffic through the BlackBerry Infrastructure to BlackBerry UEM on port 3101.
Manage work apps	On all managed devices, work apps are apps that your organization makes available for its users. You can search the app stores directly for apps to assign to devices. You can specify whether apps are required on devices, and you can view whether a work app is installed on a device. Work apps can also be proprietary apps that were developed by your organization or by third-party developers for your organization's use.
Enforce your organization's requirements for devices	You can use a compliance profile to help enforce your organization's requirements for devices, such as not permitting access to work data for devices that are jailbroken, rooted, or have an integrity alert, or requiring that certain apps be installed on devices. You can send a notification to users to ask them to meet your organization's requirements, or you can limit users' access to your organization's resources and applications, delete work data, or delete all data on the device.
Send an email to users	You can send an email to multiple users directly from the management console. The users must have an email address associated with their account.
Create or import many user accounts with a .csv file	You can import a .csv file into BlackBerry UEM to create or import many user accounts at once. Depending on your requirements, you can also specify group membership and activation settings for the user accounts in the .csv file.
View reports of user and device information	The reporting dashboard displays an overview of your BlackBerry UEM environment. For example, you can view the number of devices in your organization sorted by service provider. You can view details about users and devices, export the information to a .csv file, and access user accounts from the dashboard.
Certificate-based authentication	You can send certificates to devices using certificate profiles. These profiles help to restrict access to Microsoft Exchange ActiveSync, Wi-Fi connections, or VPN connections to devices that use certificate-based authentication.
Manage licenses for specific features and device controls	You can manage licenses and view detailed information for each license type, such as usage and expiration. The license types that your organization uses determine the devices and features that you can manage. You must activate licenses before you can activate devices. Free trials are available so that you can try out the service.
EMM SIM-Based Licensing	EMM SIM-Based Licensing is an alternative licensing model that allows you to buy licenses from your service provider instead of from BlackBerry. This option allows you to pay for licenses for BlackBerry 10, iOS, Android, and Windows devices as part of your existing plan with your service provider. For more information about licensing, see the Licensing content.

Key features for each device type

iOS devices

Feature	Description
Run app lock mode	On iOS devices that are supervised using Apple Configurator 2, you can use an app lock mode profile to limit the device to run only one app. For example, you can limit access to a single app for training purposes or for point-of-sales demonstrations.
Device activation	You can use Apple Configurator 2 to prepare devices for activation in BlackBerry UEM. Users can activate the prepared devices without using the BlackBerry UEM Client app.
Filter web content on iOS 7 and later devices	For devices that run iOS 7.0 and later, you can use web content filter profiles to limit the websites that a user can view on a device. You can enable automatic filtering with the option to allow and restrict websites, or allow access only to specific websites.
Link Apple VPP accounts to a BlackBerry UEM domain	The Volume Purchase Program (VPP) allows you to buy and distribute iOS apps in bulk. You can link Apple VPP accounts to a BlackBerry UEM domain so that you can distribute purchased licenses for iOS apps associated with the VPP accounts.
Apple Device Enrollment Program	You can configure BlackBerry UEM to use the Apple Device Enrollment Program (DEP) so that you can synchronize BlackBerry UEM with the DEP. After you configure BlackBerry UEM, you can use the BlackBerry UEM management console to manage the activation of the iOS devices that your organization purchased for the DEP. You can use multiple DEP accounts. You can link multiple Apple DEP accounts to one BlackBerry UEM domain. For more information about configuring BlackBerry UEM and activating iOS devices that are enrolled in the DEP, see the Configuration content and the Administration content.
Support for app-based PKI solutions	Added support for app-based PKI solutions, such as Purebred, which can enroll certificates for BlackBerry Dynamics apps. You can now install the PKI app on devices and allow the latest versions of BlackBerry Dynamics apps, such as BlackBerry Work and BlackBerry Access, to use certificates enrolled through the PKI app.
Use custom payload profiles	You can use custom payload profiles to control features on iOS devices that are not controlled by existing BlackBerry UEM policies or profiles. You can create Apple configuration profiles using Apple Configurator and add them to BlackBerry UEM custom payload profiles. You can assign the custom payload profiles to users, user groups, and device groups.

Feature	Description
BlackBerry Secure Gateway	The BlackBerry Secure Gateway allows iOS devices with the MDM controls activation type to connect to your work email server through the BlackBerry Infrastructure and BlackBerry UEM. If you use the BlackBerry Secure Gateway, you don't have to expose your mail server outside of the firewall to allow users with these devices to receive work email when they are not connected to your organization's VPN or work Wi-Fi network.
Integration with BlackBerry Dynamics	You can use the BlackBerry Dynamics profile to allow iOS devices to access BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. You can assign the BlackBerry Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps. The profile allows you to enable BlackBerry Dynamics for users that are not already BlackBerry Dynamics enabled.
Per-app VPN	You can set up per-app VPN for iOS devices to specify which apps on devices must use a VPN for their data in transit. Per-app VPN helps decrease the load on your organization’s VPN by enabling only certain work traffic to use the VPN (for example, accessing application servers or webpages behind the firewall). This feature also supports user privacy and increases connection speed for personal apps by not sending the personal traffic through the VPN. For iOS devices, apps are associated with a VPN profile when you assign the app or app group to a user, user group, or device group.
Apple Activation Lock	The Activation Lock feature on iOS 7 and later devices requires the user's Apple ID and password before a user can turn off Find My iPhone, erase the device, or reactivate and use the device. You can bypass the activation lock to give a COPE or COBO device to a different user.
Personal app lists	You can view a list of apps that are installed in a user's personal space on iOS devices in your environment. You can view a list of personal apps installed on a user’s device on the User Details page or view a list of all personal apps installed in users’ personal spaces on the Personal apps page in the management console.
Lost Mode for supervised iOS devices	Lost Mode allows you to lock a device, set a message that you want to display, and view the current location of the lost device. You can enable Lost Mode for supervised iOS devices running iOS 9.3 or later.
IBM Notes Traveler support	iOS devices can now connect to IBM Notes Traveler through the BlackBerry Secure Gateway.
Face ID support	BlackBerry UEM supports Face ID for device authentication and to open BlackBerry Dynamics apps.

Feature	Description
Shared device management	You can allow multiple users to share an iOS device. You can customize terms of use that users must accept to check out shared devices. A user can check out a device using local authentication and when they are done using it, they can check it in and the device is available for the next user. Shared devices remain managed by BlackBerry UEM during the check-out and check-in process. This feature was designed for supervised devices with the following configuration: • App lock mode enabled • VPP apps assigned

Android devices

Feature	Description
Manage devices using Android MDM	Android MDM uses the basic management options that are native to the Android OS to manage the device. A separate, protected container is not created. For more information about managing devices using Android MDM, see the Administration content.
Manage devices using KNOX MDM and KNOX Workspace	BlackBerry UEM can manage Samsung devices using Samsung KNOX MDM and Samsung KNOX Workspace. KNOX Workspace provides an encrypted, password-protected container on a Samsung device that includes your work apps and data. It separates a user's personal apps and data from your organization's apps and data and protects your apps and data using enhanced security and management capabilities that Samsung developed. When a device is activated, BlackBerry UEM automatically identifies whether the device supports KNOX. In addition to the standard Android management capabilities, BlackBerry UEM includes the following management capabilities for devices that support KNOX: • An enhanced set of IT policy rules • Enhanced application management including silent app installations and uninstallations, silent uninstallations of restricted apps, and prohibitions to installing restricted apps • App lock mode For more information about supported devices, see the Compatibility matrix. For more information about KNOX, visit https://www.samsungknox.com. For more information about managing devices using KNOX, see the Administration content.
Manage Android Enterprise devices	You can activate Android devices that run Android OS 5.1 or later to use Android Enterprise which is a feature developed by Google that provides additional security for organizations that want to manage Android devices and allow their data and apps on Android devices. For more information about managing Android Enterprise devices, see the Administration content.

Feature	Description
Integration with BlackBerry Dynamics	You can use the BlackBerry Dynamics profile to allow Android devices to access BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. You can assign the BlackBerry Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps. The profile allows you to enable BlackBerry Dynamics for users that are not already BlackBerry Dynamics enabled.
Per-app VPN	You can enable per-app VPN for Android devices that have a work profile to restrict the use of BlackBerry Secure Connect Plus to specific work space apps that you add to an allowed list.
Zero-touch enrollment	BlackBerry UEM supports only devices running Android 8.0 or later, that have been enabled for zero touch enrollment. Zero-touch enrollment offers a seamless deployment method for organization-owned Android devices making large-scale device deployment fast, easy, and secure for the organization and employees. Zero-touch enrollment makes it simple for IT administrators to configure devices online and have enforced management ready when employees receive their devices. See the information from Google: Zero-touch enrollment management, and the zero-touch enrollment overview information. You can get started with zero-touch enrollment in just a few steps: purchase devices, assign the devices to users, configure policies for your organization, and deploy the devices to users. You need to work with your reseller or carrier to get access to the Zero-touch portal and get devices configured in the portal.
Support for app-based PKI solutions	Added support for app-based PKI solutions, such as Purebred, which can enroll certificates for BlackBerry Dynamics apps. You can now install the PKI app on devices and allow the latest versions of BlackBerry Dynamics apps, such as BlackBerry Work and BlackBerry Access, to use certificates enrolled through the PKI app.
Android SafetyNet	When administrators enable Android SafetyNet attestation, BlackBerry UEM sends challenges to test the authenticity and integrity of Android devices that have been activated with the Android Enterprise, Samsung KNOX, and MDM controls activation types in your organization's environment.
Derived smart credentials	Use Entrust IdentityGuard derived smart credentials for signing, encryption, and authentication for BlackBerry Dynamics apps and apps in the work space on Android work profile and Samsung KNOX Workspace devices.
Factory reset protection for Android Enterprise device	You can set up a Factory reset protection profile for your organization’s Android Enterprise devices that have been activated using the Work space only activation type. This profile allows you to specify a user account that can be used to unlock a device after it has been reset to factory settings or remove the need to sign in after the device has been reset to factory settings.

Windows devices

Feature	Description
Support for Windows 10 devices	You can manage Windows 10 devices, including Windows 10 Mobile devices and Windows 10 tablets and computers. Silver licenses are required to activate Windows 10 devices.
Proxy support for Windows 10 devices	You can configure VPN and Wi-Fi work connections for Windows 10 devices and you can set up a proxy server as part of the Wi-Fi profile for Windows 10 Mobile devices.
Per-app VPN	You can set up per-app VPN for Windows 10 devices to specify which apps on devices must use a VPN for their data in transit. Per-app VPN helps decrease the load on your organization’s VPN by enabling only certain work traffic to use the VPN (for example, accessing application servers or webpages behind the firewall). This feature also supports user privacy and increases connection speed for personal apps by not sending the personal traffic through the VPN. For Windows 10 devices, apps are added to the app trigger list in the VPN profile.
Windows Information Protection for Windows 10 devices	You can configure Windows Information Protection profiles to separate personal and work data on devices, prevent users from sharing work data outside of protected work apps or with people outside your organization, and audit inappropriate data sharing practices. You can specify which apps are protected and trusted to create and access work files.

BlackBerry 10 devices

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

Compatibility and requirements

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

Product documentation

Resource	Description
Overview and what's new	• Introduction to BlackBerry UEM and its features • What's new
Architecture and data flows	• Architecture • Descriptions of BlackBerry UEM components • Descriptions of activation and other data flows, such as configuration updates and email, for different types of devices
Release notes and advisories	• Descriptions of fixed issues • Descriptions of known issues and potential workarounds • What's new
Installation and upgrade	• System requirements • Installation instructions • Upgrade instructions
Planning	• Planning BlackBerry UEM deployment for an installation or an upgrade from BES5 or BES10
Licensing	• Instructions to obtain, activate, and manage licenses • Descriptions of different types of licenses • Instructions for activating and managing licenses
Configuration	• Instructions for how to configure server components before you start administering users and their devices • Instructions for migrating data from an existing BES10 or BlackBerry UEM database
Administration	• Basic and advanced administration for all supported device types, including BlackBerry 10 devices, iOS devices, macOS computers, Android devices, Windows devices and BlackBerry OS (version 5.0 to 7.1) and earlier devices • Instructions for creating user accounts, groups, roles, and administrator accounts • Instructions for activating devices • Instructions for creating and assigning IT policies and profiles • Instructions for managing apps on devices • Descriptions of profile settings • Descriptions of IT policy rules for BlackBerry 10 devices, iOS devices, macOS computers, Android devices, Windows devices and BlackBerry OS (version 5.0 to 7.1) and earlier devices

Resource	Description
Security	• Description of device security features • Description of how you can use BlackBerry UEM to manage device security features such as encryption, passwords, and data wiping • Description of how BlackBerry UEM protects your data in transit between devices, the BlackBerry Infrastructure, BlackBerry UEM, and your organization's resources
Compatibility matrix	• List of supported operating systems, database servers, and browsers for the BlackBerry UEM server • List of supported Samsung KNOX operating systems • List of supported Android operating systems
BlackBerry enterprise products	• Descriptions of BlackBerry products such as BlackBerry UEM, BlackBerry UEM Cloud, Strong Authentication by BlackBerry, Enterprise Identity by BlackBerry, and BlackBerry Workspaces

Legal notice

GOOD and EMBLEM Design 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.

Android, Google, Google Apps, Google Play, and SafetyNet are trademarks of Google Inc. Apple Configurator, App Store, and macOS are trademarks of Apple Inc. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Box is including without limitation, either a trademark, service mark or registered trademark of Box, Inc. Cisco ISE and Cisco WebEx are trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. IBM, IBM Notes Traveler, and Domino are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Entrust IdentityGuard is a trademark of Entrust, Inc. Samsung KNOX and KNOX are trademarks of Samsung Electronics Co., Ltd. Microsoft, Active Directory, ActiveSync, Intune, Microsoft SharePoint, Windows, Windows Mobile, and Windows Phone are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Salesforce is a trademark of salesforce.com, inc. and is used here with permission. Vuzix is a trademark of Vuzix Corporation. Wi-Fi is a trademark of the Wi-Fi Alliance. Workday is a trademark of Workday, Inc. 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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada