Overview and What's New Guide

BlackBerry UEM

Version 12.7 Maintenance Release 2

Published: 2017-12-01
SWD-20171128125842999

Contents

About this guide 4

What's new in BlackBerry UEM 5

What's new in BlackBerry UEM version 12.7 MR2 5

What's new in the BlackBerry UEM 12.7 MR2 REST APIs 7

What's new in BlackBerry UEM version 12.7 MR1 7

What's new in BlackBerry UEM 12.7 9

What's new in the BlackBerry UEM 12.7 REST APIs 14

What is BlackBerry UEM? 19

BlackBerry Enterprise Mobility Suite services 19

Benefits of BlackBerry Workspaces 21

Benefits of BlackBerry Enterprise Identity 21

Benefits of BlackBerry 2FA 21

Key BlackBerry UEM features 22

Key features for all device types 25

Key features for each device type 28

Comparing BlackBerry UEM with previous EMM solutions from BlackBerry 32

Product documentation 33

Glossary 35

Legal notice 37

About this guide

1

BlackBerry UEM helps you manage iOS, Android, Windows, and BlackBerry devices for your organization.

This guide contains an overview of BlackBerry UEM, including its current features, new features, and describes which resources to consult for more in-depth information.

This guide is intended for senior IT professionals who are responsible for evaluating the product as well as anyone who is interested in learning more about BlackBerry UEM. After you read this guide, you should understand the product's capabilities and the full set of technical resources available.

What's new in BlackBerry UEM

2

This section contains a list of all the new features that have been introduced in BlackBerry UEM 12.7 and its maintenance releases.

What's new in BlackBerry UEM version 12.7 MR2

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. This option is supported only for iOS devices.

Multiple Apple Device Enrollment Program (DEP) account

Added support for using multiple DEP accounts. If you have upgraded to BlackBerry UEM 12.7 MR2 and want to configure multiple DEP accounts, you must enable the feature. If you have installed BlackBerry UEM for the first time, the feature is enabled by default.

Google account user management

New controls prevent users from adding additional accounts in the Android workspace.

Android activation

Several changes have been made to the Android activation experience including more robust explanation about password requirements, the BlackBerry UEM Client is locked into the foreground during activation, and on several screens the back button has been removed.

New IT policy rules

Group name	Display name	Description
Android work profiles	Allow changing Wi-Fi settings	Specify whether the user can change the settings in the work Wi-Fi profile. If this rule is not selected, the user

Group name	Display name	Description
		can't change any settings in the profile, including their Wi-Fi connection credentials.
Android work profiles	Allow additional Google accounts	Specify whether the user can add additional Google accounts to the work space.
Android work profiles	Disallowed account types	Specify the types of accounts that cannot be added to the work space. If no account types are specified, there is no restriction. For more information, visit http://support.blackberry.com/kb/ to read article KB46860.
Android work profiles	Allow NFC trust agent	Specify if NFC can be used to unlock the device.
Android work profiles	Allow tags with basic authentication to unlock the device	Specify if NFC tags that authenticate using the tag ID can be used to unlock the device.
Android work profiles	Allow secure NFC tags to unlock the device	Specify if NFC tags that use challenge-response authentication can be used to unlock the device.
Android work profiles	Allow Bluetooth trust agent	Specify if Bluetooth can be used to unlock the device.
Android work profiles	Allow places trust agent	Specify if places can be used to unlock the device.
Android work profiles	Allow custom places	Specify if a user can trust places other than Home.
Android work profiles	Allow Face trust agent	Specify if face image can be used to unlock the device.
Android work profiles	Allow Voice trust agent	Specify if voice can be used to unlock the device.
Android work profiles	Allow On-body trust agent	Specify if On-body can be used to unlock the device.
Android work profiles	Trust agent inactivity timeout	Specify Device inactivity timeout in minutes. When a device is in an idle state for a certain period of time, trust agents will be revoked.
Android work profiles	Allow obtaining device location	Specify if work apps can obtain location of device. This policy will supersede any location profile assigned to the user.
Android work profiles	Allow transfer of work data using NFC	Specify whether the device can send work data to another device using NFC.
KNOX MDM	Allow iris authentication	Specify whether a user can authenticate with the device using an iris scan.
KNOX MDM	Allow facial authentication	Specify whether a user can authenticate with the device using facial recognition.
KNOX Premium - Workspace	Allow iris authentication	Specify whether a user can authenticate with the work space using an iris scan.

What's new in the BlackBerry UEM 12.7 MR2 REST APIs

For details about the new additions and changes discussed here, see the *BlackBerry UEM 12.7 MR2 REST API Reference* posted here. You can view the API reference online or download it (unzip the contents and open the index file).

New paths and methods

Resource: Users

Path	Description
/{tenantGuid}/api/v1/users/{userGuid}/userDevices/{userDeviceGuid}/applications	Retrieve a list of the assigned and installed apps for a specific user device.

New data types

Type	Description
Installation status	This data type provides the installation status of an app.
User device application	This data type provides details of an assigned or installed app, including guid, disposition, status, name, version, and so on.
User device applications	This data type provides a collection of device apps.

What's new in BlackBerry UEM version 12.7 MR1

Android

Support for Android 8: BlackBerry UEM is now compatible with devices running Android 8 software.

iOS

Support for iOS 11: BlackBerry UEM is now compatible with devices running iOS 11 software.

AirPrint

AirPrint profile update : The AirPrint profile has been updated to include a checkbox that allows the administrator to force the use of TLS, and a field for specifying a port number.

Good Control to BlackBerry UEM synchronization

Improved synchronization: When upgrading from Good Control to BlackBerry UEM, Good Control can communicate with BlackBerry Dynamics containers during the synchronization process, which helps to remove the risk of downtime for end users.

Google Play and the Samsung KNOX Workspace

Support installing specific apps from Google Play in Samsung KNOX Workspace: Administrators can now specify a list of apps from the Google Play Store that users can install in the Samsung KNOX Workspace.

New IT Policy rules

Device type	Type	Description
iOS	Allow AirPrint (supervised only)	Specify whether users can use AirPrint on the device.
iOS	Allow AirPrint credentials storage (supervised only)	Specify whether users can store AirPrint credentials using iCloud Keychain.
iOS	Force trusted certificates for TLS (supervised only)	Specify whether the device must use trusted certificates with TLS to connect to printers using AirPrint.
iOS	Allow AirPrint iBeacon discovery (supervised only)	Specify whether the AirPrint app can use iBeacons to discover nearby printers.
iOS	Allow users to configure Wi-Fi settings (supervised only)	Specify whether users can configure Wi-Fi settings. If this rule is not selected, devices can only connect to Wi-Fi networks if the settings have been sent to the device by a configuration profile, for example a UEM Wi-Fi profile or using the Apple Configurator.
iOS	Allow dictation (supervised only)	Specify whether users can use dictation on the device.
iOS	Allow user-configured VPN (supervised only)	Specify whether a user can add a VPN configuration to the device.
iOS	Allow system app removal (supervised only)	Specify whether a user can remove system apps from the device.
Android	Default app permissions	Specify whether app permission requests are granted or denied by default. If you select

Device type	Type	Description
		"Prompt user" the user is asked to grant or deny permissions. If you select "Always grant" the user is not prompted and permission requests are always granted. If you select "Always deny" the user is not prompted and permissions requests are always denied.
Android	Allow lock screen features	Specify whether special features can be enabled on the device lock screen.
Android	Allow camera on lock screen	Specify whether users can access the device camera on lock screen.
Android	Allow notifications	Specify whether the device can display notifications on the lock screen.
Android	Allow all notification content	Specify whether all notification content can appear on the lock screen or only the notification type.
Android	Allow fingerprint authentication	Specify whether the user can unlock the device using a fingerprint.
Android	Allow notification responses	Specify whether the user can type a response to a notification on the lock screen.
Android	Allow trust agents	Specify whether trust agents can unlock the device.

What's new in BlackBerry UEM 12.7

This section contains a list of all the new features that have been introduced in BlackBerry UEM 12.7.

Microsoft Intune

Microsoft Intune integration: For iOS and Android devices, if you want to protect data in Microsoft Office 365 apps using the MAM features of Microsoft Intune, you can use Intune to protect app data while using BlackBerry UEM to manage the devices. Intune provides security features that protect data within apps. For example, Intune can require that data within apps be encrypted and prevent copying and pasting, printing, and using the Save as command. You can connect UEM to Intune, allowing you to manage Intune app protection policies from within the UEM management console. **Note**: The Microsoft API that allows UEM to connect to Intune is currently in Beta. Service interruptions could occur for this feature if Microsoft makes significant changes to the API. (JI 1672797)

Device management

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 codes, IT policies, app management and location services. (JI 1639423)

Apps

- **App configuration**: For Android email apps that support app configuration (such as BlackBerry Productivity Suite), you can configure the settings in an app configuration instead of in an Email profile. You must be using Android work profiles to use this feature. (JI 1667334)
- **List of installed apps**: You can specify whether BlackBerry UEM receives a list of apps that are installed in the user's personal space on iOS, Android, Windows 10, and BlackBerry 10 devices in your environment. By default, the ability to view apps that are installed in the user's personal space is enabled when the device is activated using a supported activation type. You can view the list of apps that are installed in a user's personal space in the user account's device details page or the Personal apps page. (JI 597445)

  Note: You can also view apps that were installed on devices before they were activated as KNOX Workspace only devices.

  Viewing the list of personal apps installed in the user's personal space is not supported on devices that are activated with the following activation types:

  - iOS and Android: User privacy
  - Android: Work and personal - user privacy
  - Samsung KNOX: Work and personal - user privacy - (Samsung KNOX)
  - BlackBerry 10: Work and personal - Corporate
  - iOS and Android: Device registration for BlackBerry 2FA only

- **App update notifications**: Device users are notified of any new or updated apps. There is a new "Updated/New" tab in the Work Apps list and in the Work apps section of the BlackBerry UEM Client. (JI 1457273)
- **Apple VPP account**: You can configure the VPP account to automatically update VPP apps on devices. (JI 2161425)
- **Restricted apps**: For Samsung KNOX devices activated with Work and personal - full control, you can create a compliance profile that enforces app restrictions in the personal space as well as the workspace. (JI 1355193)
- **VPP apps**: You can associate VPP licenses to iOS BlackBerry Dynamics app entitlements just as you can for other iOS apps. You can associate VPP licenses when you assign apps (or app groups) to users or user groups. (JI 1634604)

Management console

- **Bulk updates**: The following are added to the list of commands that can be sent to multiple devices: Update device information; Delete all device data; Delete only work data; Remove devices; Change device ownership; and Update OS (for supervised iOS devices. (JI 597377)
- **Upload a certificate**: User credential profiles now allow administrators or users to upload a certificate to push to devices. (JI 727068)
- **Customize the consoles**: You can add a custom background image for the log in screen, a custom logo, and a custom name for BlackBerry UEM Self-Service. (JI 1632110)
- **User certificate upload**: User credential profiles now allow users to upload certificates to BlackBerry UEM that can be associated with Wi-Fi, VPN, and email profiles. (JI 1650044)
- **Admin commands**: The Remove device command lets you remove a device from BlackBerry UEM. (JI 1650852)
- **License expiration date**: The Licensing summary page in the management console now always displays the license expiration date instead of displaying the date only within the warning period. (JI 1639127)
- **User search**: On the top right corner of the User > Managed devices screen, there is a User search link that you can use as an alternative method to search for users by name. Note that if you log out of the console when you are on the User search screen, when you log back into the console you will be returned to the User search screen. (JI 2167287)
- **Login notice**: The character limit that can be used in the login notice for the BlackBerry UEM management console and BlackBerry UEM Self-Service has been increased. The maximum number of characters is now 50,000. (JI 1696243)
- **Notes field**: A notes field has been added for users. Administrators can use the notes field to keep track of any special information about the user. This information is stored against the user object and not against an individual device. If the user is removed, the information in the notes field is also removed. (JI 892592)
- **Password complexity**: In Settings > General settings > Activation defaults, administrators can specify minimum or maximum password complexity for automatically generated activation passwords. Administrators can specify password length as well as if lowercase letters, uppercase letters, numbers, or special characters are required for the password. (JI 801154)
- **Gatekeeping profile**: You can now configure the gatekeeping servers in a gatekeeping profile instead of in an email profile. On upgrade to BlackBerry UEM 12.7, gatekeeping profiles are automatically created if you previously configured gatekeeping in email profiles. (JI 1667334)
- **User role**: A new user role setting allows you to configure whether or not users have permission to create access keys in BlackBerry UEM Self-Service. (JI 2143060)
- **Choose the BlackBerry Proxy cluster to use for activation**: Select the Enabled for activation option for the BlackBerry Proxy instance that you want to use for activation purposes. (JI 1638296)

BlackBerry UEM Self-Service

Activation password email: You can configureBlackBerry UEM Self-Service to send an activation email to users when they create activation passwords using BlackBerry UEM Self-Service. (JI 1668729)

Device activation

QR code activation: Users can activate iOS and Android devices using a QR code instead of an activation password. You can send the QR code in an activation email or users can create a QR code in BlackBerry UEM Self-Service. (JI 1639098)

Monitoring

- **Event notifications**: You can set up notifications so that emails are sent to administrators when certain events occur in BlackBerry UEM or on devices. For each event notification you can configure a recipient list, select the days and times to send notifications, and select an email template to use. (JI 930520)
- **Monitor BlackBerry Work**: You can monitor the performance of the BlackBerry Work app and choose the issues that you want to be reported. (JI 1642267)

iOS

- **Supervised devices**: You can configure the activation profile to restrict devices in BlackBerry UEM that are not in supervised mode. If you restrict unsupervised devices, users cannot activate unsupervised devices whether they activate devices with the BlackBerry UEM Client or using DEP. (JI 1584129)
- **Logging**: You can use the “Get device logs” command to retrieve device logs from iOS devices that have the BlackBerry UEM Client installed (JI 597503)
- **Update OS and other new commands**: You can send the following new commands to iOS devices. (JI 2162972)
    - Update OS (supervised DEP devices running iOS 9 and later and supervised devices running iOS 10.3 and later)
    - Restart device (supervised devices running iOS 10.3 and later)
    - Turn off device (supervised devices running iOS 10.3 and later)

Android

- **Android for Work**: The BlackBerry UEM console and documentation is updated to reflect Google's rebranding of Android for Work. (JI 1657568)
- **Logging**: You can use the “Get device logs” command to retrieve device logs from Android devices that have the BlackBerry UEM Client installed. (JI 940762)

Samsung KNOX

- **Organizational message**: You can set an organizational message to appear when the device is locked or rebooted. (JI 855979)
- **Wallpaper**: You can set the wallpaper that displays on the device and the workspace. (JI 855979)
- **Transferring contacts**: Samsung KNOX Workspace devices support transferring contacts using the Bluetooth Phone Book Access Profile. This capability can be disabled by an IT policy rule. (JI 1613041)

Windows 10

- **App mode profile**: You can use an app lock mode profile to limit Windows 10 Enterprise and Windows 10 Education devices managed using MDM to run only one app. For example, you can limit access to a single app for training purposes or for point-of-sales demonstrations. (JI 691076)
- **SCEP profile**: Administrators can now select a SCEP profile to associate with a Wi-Fi profile for Windows 10 devices. (JI 990153)
- **FIPS mode and AutoConnect**: Administrators can now enable FIPS mode and AutoConnect for Windows 10 devices in a Wi-Fi profile. FIPS mode can be enabled when WPA2-Personal or WPA2-Enterprise security type and the AES encryption type are selected. Administrators may choose to allow the device to connect automatically to the Wi-Fi network when it is in range. (JI 729800)
- **Reboot**: Administrators can now reboot a Windows 10 Mobile device running RS1 and later from the BlackBerry UEM console. (JI 1657059)
- **Windows Information Protection profile**: Administrators can now configure additional options in Windows Information Protection profiles. For example, you can configure the work IP ranges that are considered to be part of the work network, any internal proxy servers to use when connecting to work network locations, and cloud resources that need to be protected, and a list of domains that can be used for work or personal resources. (JI 1451930)
- **Lock Down setting**: Administrators can now enable the Lock Down setting in VPN profiles for Windows 10 devices. When this setting is enabled, the device stays connected to the VPN, must be connected to have a network connection, and cannot be disabled. (JI 1634629)

Device management

Apple TV: You can activate and manage Apple TV devices in BlackBerry UEM. (JI 1603242)

BlackBerry Dynamics

- **Certificates**: BlackBerry Dynamics apps now support replacing certificates issued by BlackBerry Control with certificates issued by another CA. (JI 1673783)
- **PKI connector enhancements**: User credential profiles now allow you to set certificate renewal and revocation options for certificates issues to users through the BlackBerry Dynamics PKI connector. (JI 1625882)

BlackBerry Dynamics Launcher

Shortcuts: You can add shortcuts to the BlackBerry Dynamics Launcher so that users can quickly access web links. (JI 1430992)

BlackBerry Dynamics SDK

No password required: With a security policy enforced by the BlackBerry Dynamics SDK and BlackBerry UEM, enterprises can allow users to start mobile applications without requiring a password. The “No Password” feature is available on iOS, Android, macOS, and Windows 10 (UWP). (JI 1430992)

Policy rules

New policy rules were added for BlackBerry UEM 12.7. To see the new rules, in the BlackBerry UEM Policy Reference Spreadsheet, in the 'Introduced in BES12/BlackBerry UEM Version' column click the arrow and select 12.7.0.

What's new in the BlackBerry UEM 12.7 REST APIs

For details about the new additions and changes discussed here, see the *BlackBerry UEM 12.7 REST API Reference* posted here. You can view the API reference online or download it (unzip the contents and open the index file).

New paths and methods

Resource: Devices

Path	Description
GET /{tenantGuid}/api/v1/devices	Search for devices.

Resource: Groups

Path	Description
POST /{tenantGuid}/api/v1/groups/{groupGuid}/users	Add user accounts to a user group by GUID.
POST /{tenantGuid}/api/v1/groups/{groupGuid}/applications	Assign apps to a user group by GUID.
POST /{tenantGuid}/api/v1/groups	Create a user group.
DELETE /{tenantGuid}/api/v1/groups/{groupGuid}	Delete a user group.
DELETE /{tenantGuid}/api/v1/groups/{groupGuid}/users	Remove user accounts from a user group by GUID.
DELETE /{tenantGuid}/api/v1/groups/{groupGuid}/applications/{appGuid}	Remove an app from a user group by GUID.

Resource: Info

Path	Description
GET /{tenantGuid}/api/v1/info/systeminfo	Get system info.

Resource: Users

Path	Description
GET /{tenantGuid}/api/v1/users/{userGuid}	Get the details of a user account by GUID.
PATCH /{tenantGuid}/api/v1/users/{userGuid}	Update the password for a local (non-directory) user.
GET /{tenantGuid}/api/v1/users/{userGuid}/applications	Get all apps that are directly assigned to a user account.
GET /{tenantGuid}/api/v1/users/{userGuid}/groups	Get all user groups that a user account is assigned to.
GET /{tenantGuid}/api/v1/users/{userGuid}/services	Get the services that are assigned to a user account.
DELETE /{tenantGuid}/api/v1/users/{userGuid}	Remove the specified user account.
GET /{tenantGuid}/api/v1/users/{userGuid}/userDevices	Get the devices that are assigned to a user account.
GET /{tenantGuid}/api/v1/users/{userGuid}/userDevices/{userDeviceGuid}	Get a specific device that is assigned to a user account.
PUT /{tenantGuid}/api/v1/users/{userGuid}/profiles/{profileGuid}/certificate	Add or update a certificate for a user credential profile that supports manually uploaded certificates.
DELETE /{tenantGuid}/api/v1/users/{userGuid}/profiles/{profileGuid}/certificate	Remove a manually uploaded certificate from a user credential profile.

New data types

Type	Description
Application assignment	An app that is (or can be) assigned to a user account or user group
Application assignments	A collection of app assignments
Certificate	A certificate that is defined in BlackBerry UEM
Device	A device that is defined in BlackBerry UEM
Devices	A collection of devices
Email template types	The types of email templates that are supported
Enrollment types	The device enrollment types that are supported
Link	A link related to a resource; for example, a link between a user and the groups and profiles the user is associated with

Type	Description
Profile categories	Profile categories that are supported
Service	Represents a service; for example, MDM (Mobile Device Management) is a service that can be associated with a user so that an administrator can manage the user's devices
Service assignment	Represents a service that can be assigned
Service assignment statuses	The service assignment statuses that are supported
Service assignments	A collection of service assignments
SystemInfo	System information; for example, activation URL, management console URL, product version, and so on
User custom variable	A custom variable that is set for a user account
User detail	The details of a user account
User device	A user's device that is defined in BlackBerry UEM
User devices	A collection of user devices

Changes to resources

Resource: Users

In the previous release, the following were organized under the **Activation passwords** resource. In this release, they have been moved into the **Users** resource:

Path	Description
GET /{tenantGuid}/api/v1/users/{userGuid}/activationPasswords	Get all of the non-expired activation passwords for a user account.
POST /{tenantGuid}/api/v1/users/{userGuid}/activationPasswords	Set one or more activation passwords for a user account.
PUT /{tenantGuid}/api/v1/users/{userGuid}/activationPasswords	Replace all of the activation passwords for a user account.
DELETE /{tenantGuid}/api/v1/users/{userGuid}/activationPasswords	Expire all of the activation passwords for a user account.

Path	Description
DELETE /{tenantGuid}/api/v1/users/{userGuid}/activationPasswords/{activationPasswordGuid}	Expire a specific activation password for a user account.

The following request parameters have been added to **GET /{tenantGuid}/api/v1/users**:

Parameter	Description
includeTotal	Used to retrieve the total number of user accounts that match the search criteria, which may be different from the number of user accounts returned.
max	The maximum number of user accounts to return, between 1 and 1000. The default value is 100.
offset	The number of user accounts to exclude from the beginning of the search results, greater than or equal to 0. Used to get pages of results, for example, with max=50 and offset=0 for the first 50 users, max=50 and offset=50 for the next 50 users, and so on. The default value is 0.
sortBy	The field to sort the results by.

For **GET /{tenantGuid}/api/v1/users**, the following fields have been added to the query request parameter:

- displayName
- guid
- directoryId
- groupGuid
- profileGuid

For **POST /{tenantGuid}/api/v1/users**, additional information has been added to the API reference to indicate the fields that are allowed when creating a directory-linked user or a local user, and information has been added about the Location response header.

For **POST /{tenantGuid}/api/v1/users/{userGuid}/activationPasswords** and **PUT /{tenantGuid}/api/v1/users/{userGuid}/activationPasswords**, the following response code has been added:

- 503: SMTP server temporarily unavailable to send emails. Retry the request again later.

Changes to data types

Data type	Changes
Email template	A **default** property has been added to indicate whether it is the default email template.
Profile	A **default** property has been added indicate whether it is the default profile for that category.

Data type	Changes
User	A **links** property has been added to indicate links from a user to related resources, for example, groups and profiles.
Users	A **total** property has been added to indicate the total number of users that match the search criteria, which may be different from the number of user accounts returned.

What is BlackBerry UEM?

3

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 Enterprise Identity, and BlackBerry 2FA that allow you to add value to your BlackBerry UEM Cloud 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

Service type	Service name and description
	files by applying DRM controls to limit access, even after they are shared with someone outside of your organization. • BlackBerry Enterprise Identity gives users single sign-on access to service providers such as BlackBerry Workspaces, Box, Workday, WebEx, Salesforce, and more. You can also add support for custom SaaS services. • BlackBerry 2FA protects access to your organization's critical resources using two-factor authentication. BlackBerry 2FA uses a password that users enter and a secure prompt on their Android, iOS, or BlackBerry 10 devices each time they attempt to access resources.
BlackBerry Dynamics platform	• The BlackBerry Enterprise Mobility Server (BEMS) 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 Share allows users to securely access, download, and share documents by integrating Microsoft SharePoint and other work repositories with 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.

Service type	Service name and description
	• 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.

Key BlackBerry UEM features

4

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. You can manage the WorkLife by BlackBerry plug-in in the BlackBerry UEM management console. WorkLife by BlackBerry is a Virtual SIM Platform (VSP) that allows you to separate work numbers and personal numbers on BlackBerry 10, iOS, and Android devices. For more information on installing and managing WorkLife in BlackBerry, see the WorkLife by BlackBerry content.
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,

Feature	Description
	deleting device data, or lock their lost or stolen devices, and address other critical support requirements.
Integration with services such as BlackBerry Workspaces, BlackBerry Enterprise Identity, and BlackBerry 2FA	You can integrate BlackBerry UEM with BlackBerry Workspaces, BlackBerry Enterprise Identity, and BlackBerry 2FA that allow you to add value to your organization's BlackBerry UEM instance.
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.

Feature	Description
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.
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 Service, 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. **Note**: The Microsoft API that allows UEM to connect to Intune is currently in Beta. Service interruptions could occur for this feature if Microsoft makes significant changes to the API.

Key features for all device types

5

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.

Feature	Description
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.
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

Feature	Description
	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

6

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. For more information about configuring BlackBerry UEM and activating iOS devices that are enrolled in the DEP, see the Configuration 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. This option is supported only for iOS devices
Use custom payload profiles	You can use custom payload profiles to control features on iOS devices that are not controlled by existing BlackBerry UEM policies or profiles. You can create Apple configuration profiles using Apple Configurator and add them to BlackBerry UEM custom payload profiles. You can assign the custom payload profiles to users, user groups, and device groups.
BlackBerry Secure Gateway Service	The BlackBerry Secure Gateway Service 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 Service, you don't have to expose

Feature	Description
	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 Service.

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.

Feature	Description
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 devices that use Android work profiles	You can activate Android devices that run Android OS 5.1 or later to use Android work profiles. Android work profiles are 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 devices using Android work profiles, see the Administration content.
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.

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.

Feature	Description
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.

Comparing BlackBerry UEM with previous EMM solutions from BlackBerry

7

EMM solution	Supported device types	Description
BlackBerry UEM	• BlackBerry 10 • BlackBerry OS (version 5.0 to 7.1) • iOS (including DEP devices) • macOS • Android (including devices that use a work profile and Samsung KNOX) • Windows Phone • Windows 10 • Windows 10 Mobile	A multiplatform EMM solution that allows you to manage the server, user accounts, and all device types with a single UI. This simple, web-based management console allows you to manage BYOD, COPE, and COBO devices and protect business information. The software architecture has been simplified for easier management, increased scalability, and additional multiplatform features. For high availability, you can install additional active servers that share the management load automatically. Note that to manage BlackBerry (version 5.0 to 7.1) devices with BlackBerry UEM, you must upgrade from BES5 to BlackBerry UEM.
BES10	• iOS • Android • BlackBerry 10 • BlackBerry OS (version 5.0 to 7.1)	You can manage the server, devices, and user accounts with dedicated, advanced UIs for different device types. You can also use BlackBerry Management Studio as a single, unified UI for basic administration of all devices. For high availability, you can install standby instances of the server. To manage BlackBerry OS (version 5.0 to 7.1) devices, you can install BES10 on the same computer as BlackBerry Enterprise Server 5.0 SP4 and use BlackBerry Management Studio for basic administration.
BES5 5	• BlackBerry OS (version 5.0 to 7.1)	You can manage the server, devices, and user accounts with the BlackBerry Administration Service. For high availability, you can install standby instances of most server components.

Product documentation

8

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

Resource	Description
	• 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
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
FAQs	• Answers to frequently asked questions on several subject such as administration, licensing, and certificates
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

Glossary

9

BES5	BlackBerry Enterprise Server 5
BES10	BlackBerry Enterprise Service 10
BYOD	bring your own device
COBO	corporate-owned, business only
COPE	corporate-owned, personal enabled
EMM	Enterprise Mobility Management
IP	Internet Protocol
IT policy	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.
KDC	A Key Distribution Center (KDC) is a server that performs the trusted arbitrator role for the Kerberos protocol. The KDC issues service tickets and maintains a list of tickets that it issued. Domain controllers are KDCs.
LDAP	Lightweight Directory Access Protocol
MDM	mobile device management
PGP/MIME	PGP Multipurpose Internet Mail Extensions
MMS	Multimedia Messaging Service
QoS	Quality of Service
SaaS	Software as a Service
SCEP	simple certificate enrollment protocol
SIM	Subscriber Identity Module
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UEM	Unified Endpoint Manager
VPN	virtual private network
VPP	Volume Purchase Program

VSP	virtual SIM platform
XML	Extensible Markup Language

Legal notice

10

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