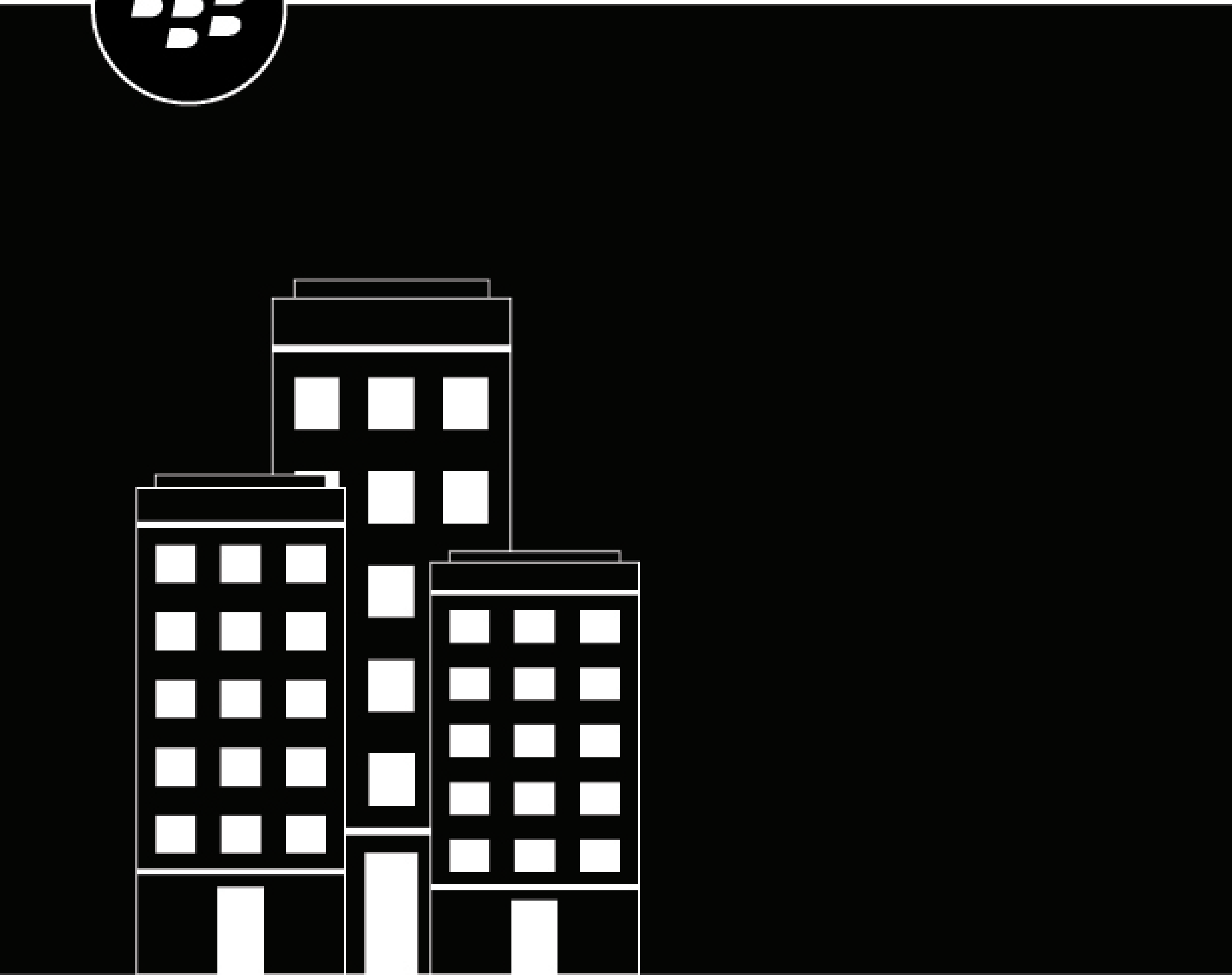

# BlackBerry UEM

## Overview and What's New

12.11

# Contents

# What's new in BlackBerry UEM 12.11 MR1

### BlackBerry Intelligent Security

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

### Android

- **Apply security patch level enforcement to BlackBerry Dynamics apps on Android devices**: In a compliance profile you can apply security patch level enforcement to BlackBerry Dynamics apps. If the security patch level is not met, you can choose to delete the BlackBerry Dynamics app data, not allow BlackBerry Dynamics apps to run on the device, or perform no actions on the device.
- **Compliance policy update**: A new compliance setting allows administrators to enable or disable anti-debugging for BlackBerry Dynamics apps. If your organization prohibits turning off detection for rooted OS or failed attestation, you can use this setting to disable the anti-debugging check without disabling rooted OS or failed attestation detection.
- **User notifications**: Updates to Android 10 required changes to the BlackBerry UEM Client to use notifications instead of pop-up dialog boxes to inform users of events and request user input. Users must allow notifications from the UEM Client to avoid unexpected behavior.
- **UEM Client native library updates:** The BlackBerry UEM Client for Android native libraries have been updated to support a 64-bit architecture.
- **BlackBerry Connectivity native library updates:** The BlackBerry Connectivity app for Android native libraries have been updated to support a 64-bit architecture.

### iOS

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

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

### Samsung Knox

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

### MDM Controls activation type

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

### SHA1

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

### APNs

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

### IT Policy Rule updates

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

# Whats new in BlackBerry UEM 12.11

### Security

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

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

### Management Console

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

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

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

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

#### Activation

- **Activate Android Enterprise devices without adding a Google account**: Administrators now have the option to allow Android Enterprise devices to be activated without adding a Google Play account to the workspace. You might use this option if you do not want to use Google Play to manage work apps on Android Enterprise devices or you want to activate and use the device without accessing Google services. In the activation profile, you specify whether to add Google Play to the workspace for Android Enterprise devices. By default, the activation profile adds the Google account to the work space and Google Play manages the apps. If you do not add a Google account, apps and app configurations are managed through the BlackBerry UEM infrastructure via BlackBerry UEM Client.
- **BlackBerry UEM now includes Work and personal – full control activations for Android Enterprise devices**: This activation type is for devices running Android 8 and later. It lets you manage the entire device. It creates a work profile on the device that separates work and personal data but allows your organization to maintain full control over the device and wipe all data from the device. Data in both the work and personal profiles is protected using encryption and a method of authentication such as a password. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files.

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

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

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

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

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

### Windows 10 Modern Management

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

### Intune

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

### Apple Configurator

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

### BlackBerry Dynamics

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

### Logging

- **Logging changes:** The BlackBerry UEM administrator console includes the following changes for logging:
    - You can now enable SQL logging, CAP payload logging, and HTTP payload logging. These options are available under Settings > Infrastructure > Logging.
    - The Maximum device app audit log file size is now configured as a global setting instead of per instance. If you upgrade from a previous release, the maximum size is initially set to the minimum setting for any existing server instance.
    - Component level logging is now supported for BlackBerry Proxy Service. You can enable logging for BlackBerry Proxy Service under Settings > Infrastructure > Logging, as well as the Server group and BlackBerry Connectivity Node default settings pages.

- **Trace logging option removed:** The option to set logging level to Trace has been removed from Service logging override. You can set logging level to Info, Error, Warning, or Debug.
- **BlackBerry Proxy Service:** Component level logging is now available for BlackBerry Proxy Service. You can enable logging for BlackBerry Proxy Service on the Server group and BlackBerry Connectivity Node default settings pages.

### BlackBerry Connectivity

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

### BlackBerry Web Services

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

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

### Changes to the Planning and the Installation and Upgrade content

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

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

### New IT policy rules

#### iOS

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

| | |
|---|---|
| Allow sending Siri logs to Apple | Specify whether the device can send Siri logs to Apple servers. |

**Android Enterprise (Global)**

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

**Android Enterprise (Work profile)**

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

**Android Enterprise (Personal profile)**

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

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

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

# What is BlackBerry UEM?

BlackBerry UEM is a multiplatform EMM solution from BlackBerry that provides comprehensive device, app, 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.

Benefits of BlackBerry UEM include:

| 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 plus additional BlackBerry Secure UEM & Productivity Suite services 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 setup and enrollment | Allow users to activate their own devices with BlackBerry UEM Self-Service. |
| Industry-leading mobile security | Leverage the BlackBerry Infrastructure to ensure data security across all 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, BlackBerry 2FA, BBM Enterprise, 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 services

Beyond the security and productivity features that BlackBerry UEM provides, BlackBerry offers more services that can add value to your BlackBerry UEM 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.<br>• 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.<br>• 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.<br>• 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) on-premises and BEMS-Cloud provides additional services for BlackBerry Dynamics apps.<br>  • BEMS on-premises integrates the BlackBerry Mail, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs services. When these services are integrated, users can communicate with each other using secure email messages and instant messaging, view the real-time presence of users in BlackBerry Dynamics apps, and access, synchronize, and share work file server, Microsoft SharePoint, Microsoft SharePoint Online, Microsoft OneDrive for Business, and Box documents without putting work data at risk.<br>  • BEMS-Cloud integrates the BlackBerry Mail and BlackBerry Docs services. When these services are integrated, users can communicate with each other using secure email messages and access, synchronize, and share Microsoft SharePoint, Microsoft SharePoint Online, Microsoft OneDrive for Business, and Box documents without putting work data at risk.<br>• The BlackBerry Dynamics SDK allows developers to create secure apps for Android and iOS devices and Mac OS and Windows computers. |

| Service type | Service name and description |
|---|---|
| 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.<br>• BlackBerry Access enables users to securely access their organization's intranet with their device.<br>• 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.<br>• BlackBerry Tasks allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their Android and iOS devices.<br>• BlackBerry Notes allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their device. |

These services can be purchased as part of a BlackBerry Secure UEM & Productivity Suite license. For more information about the different BlackBerry Secure UEM & Productivity Suite licenses and how to obtain them, see the Licensing content.

# BlackBerry Secure UEM & Productivity Suites

BlackBerry Secure UEM & Productivity Suites include BlackBerry UEM, BlackBerry Dynamics, and additional services under one license to offer a comprehensive unified endpoint management solution that provides mobile collaboration and a trusted end-to-end approach to security.

| Suite | Features |
|---|---|
| BlackBerry Secure UEM & Productivity Suites – Choice Suite | • Cross-platform support for iOS, macOS, Android (including Samsung Knox), Windows 10, and BlackBerry 10 devices<br>• BlackBerry UEM with support for Work and personal - Corporate activations for BlackBerry 10 devices, MDM controls for most device types, User privacy activations for iOS and Android devices, and Work and personal and Work space only activations for Android devices<br>• BlackBerry Dynamics with support for MDM, MAM, BlackBerry Access, and BlackBerry Work<br>• Secure instant messaging using BlackBerry Connect<br>• Cloud and on-premises deployment options<br>• Data gathering and usage metrics from BlackBerry Dynamics apps on your users' devices using BlackBerry Analytics |

| Suite | Features |
|---|---|
| BlackBerry Secure UEM & Productivity Suites – Freedom Suite | • All BlackBerry Secure UEM & Productivity Suites – Choice Suite features<br>• Advanced BlackBerry UEM security and connectivity features for managing iOS, Android (including Samsung Knox Workspace and Knox Platform for Enterprise), and BlackBerry 10 devices<br>• Secure access to work content using BlackBerry Secure Connect Plus and BlackBerry Docs<br>• Unlimited deployment of BlackBerry Dynamics secured apps from third-party software vendors<br>• Secure access to view, edit, and save documents using Intune managed Microsoft apps, such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel, in BlackBerry Dynamics apps on iOSand Android devices using BlackBerry Enterprise BRIDGE<br>• Complete cloud service federation and single sign-on solution using BlackBerry Enterprise Identity<br>• Unlimited deployment of customer-developed BlackBerry Dynamics secured apps<br>• Custom shared services app integration<br>• Full two-factor authentication enabled through users' devices with BlackBerry 2FA<br>• Enterprise file synchronization, sharing, and access control with BlackBerry Workspaces |
| BlackBerry Secure UEM & Productivity Suites – Limitless Suite | • All BlackBerry Secure UEM & Productivity Suites – Freedom Suite features<br>• Send messages to users via SMS, phone, and email directly from the BlackBerry UEMmanagement console with UEM Notifications<br>• Enterprise file synchronization, sharing, access control, document rights management across mobile devices, and SDK support with BlackBerry Workspaces |

## Benefits of BlackBerry Workspaces

BlackBerry Workspaces is an enterprise file management platform that allows users to securely access, synchronize, edit, and share files and folders across multiple devices. BlackBerry Workspaces limits the risk for data loss or theft by embedding digital rights management security into every file, so your content remains secure and within your control, even after it is downloaded and shared with others. 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.

Users can access BlackBerry Workspaces from a Web browser and from apps on Windows and macOS computers and on iOS, Android, and BlackBerry 10 devices. Content is synchronized across all of a user's devices when they are online, allowing users to manage, view, create, edit, and annotate files from any device. You can use the Workspaces plug-in for BlackBerry UEM to integrate Workspaces management into the BlackBerry UEM management console

If your organization also implements BlackBerry Enterprise Identity, you can use Enterprise Identity to manage user entitlement to Workspaces. For more information about Enterprise Identity see the BlackBerry Enterprise Identity content.

BlackBerry Workspaces can be purchased separately or licensed with BlackBerry Secure UEM & Productivity Suites – Freedom Suite. Additional features are included with BlackBerry Secure UEM & Productivity Suites – Limitless Suite.

For more information, see the BlackBerry Workspaces content.

## 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 10, 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 provides single sign-on (SSO) to cloud services such as Microsoft Office 365, G Suite, BlackBerry Workspaces, and many others. With single sign-on, users don't have to complete multiple log ins or remember multiple passwords. Administrators can also add custom services to Enterprise Identity to give users access to internal applications.

Administrators use the BlackBerry UEM management console to add services, manage users, and to add and manage additional administrators. The integration with BlackBerry UEM makes it easy to manage users and entitle them to access cloud applications and services from their devices. Using BlackBerry UEM, cloud services and mobile app binaries can be bundled together and then simply assigned to a user or group of users.

Enterprise Identity can be purchased separately or licensed with these BlackBerry Secure UEM & Productivity Suites

- Choice Suite
- Freedom Suite
- Limitless Suite

For more information about Enterprise Identity, see the BlackBerry Enterprise Identity content.

## Benefits of BlackBerry 2FA

BlackBerry 2FA provides users with two-factor authentication to access your organization’s resources. It allows you to use your users iOS, Android, BlackBerry 10, or BlackBerry OS (version 6.0 to 7.1) devices as the second factor of authentication when users connect to your organization’s resources. BlackBerry 2FA provides a simple user experience that prompts users for confirmation on their device when they attempt to access one of your resources.

For users who don't have a mobile device or have a mobile device that doesn't have sufficient connectivity to support the real-time BlackBerry 2FA, you can issue standards-based one-time password (OTP) tokens. The first authentication factor is the user's directory password, and the second authentication factor is a dynamic code that appears on the token's screen.

You manage BlackBerry 2FA from the BlackBerry UEM or BlackBerry UEM Cloud management console. BlackBerry 2FA is also integrated with BlackBerry Enterprise Identity. You can use BlackBerry 2FA to provide a second factor of authentication for the resources that you manage access to with Enterprise Identity.

BlackBerry 2FA can be purchased separately or licensed with these BlackBerry Secure UEM & Productivity Suites

- Freedom Suite
- Limitless Suite

For more information about BlackBerry 2FA, see the BlackBerry 2FA content.

## Benefits of BlackBerry UEM Notifications

BlackBerry UEM Notifications takes advantage of the BlackBerry AtHoc Networked Crisis Communication system to allow administrators can send critical messages and notifications to users and groups from the UEM management console.

Because UEM Notifications allows administrators to manage devices and notifications within the UEM management console, they don't need to 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, including 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.

BlackBerry UEM Notifications can be purchased separately with BlackBerry UEM or licensed with BlackBerry Secure UEM & Productivity Suites – Limitless Suite.

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 iOS and Android devices. Users require the BlackBerry UEM Client to activate iOS or Android devices 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:<br>• Verify whether their devices are compliant with the organization's standards<br>• View the profiles that have been assigned to their user accounts<br>• View the IT policy rules that have been assigned to their user accounts<br>• Access work apps<br>• Create access keys for BlackBerry Dynamics apps<br>• Preauthenticate with BlackBerry 2FA<br>• Access a software OTP code<br>• Retrieve and email device log files<br>• Deactivate their devices<br>For more information, see the BlackBerry UEM Client 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. For more information, see the documentation for each app. |

| Component | Description |
|---|---|
| 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.<br>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.<br>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.<br>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:

| 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.<br>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.<br>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.<br>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.<br>For more information about BlackBerry Tasks, see the BlackBerry Tasks content. |

| App | Description |
|---|---|
| BlackBerry Notes | BlackBerry Notes allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their mobile device of choice.<br>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.<br>For more information about the BlackBerry UEM Integration SDK, see the BlackBerry UEM Integration SDK content. |
| 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:<br>• Security services (for example, secure communications and interapp data exchange APIs)<br>• Mobile services (for example, presence, email, push, directory lookup)<br>• Platform services (for example, single sign-on authentication, identity and access management, app-level controls for admins)<br>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.<br>For more information about the BlackBerry Analytics SDK, see the BlackBerry Analytics content. |

| Component | Description |
|---|---|
| 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.<br>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.<br>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.<br>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 10, and BlackBerry 10 devices. BlackBerry UEM installations that have been upgraded from BES5 can also manage BlackBerry OS (versions 5.0 to 7.1) 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 Enterprise 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.<br>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.<br>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.<br>To integrate BlackBerry UEM Cloud with your company directory you must install the BlackBerry Connectivity Node. You can install one or more instances of the BlackBerry Connectivity Node. |
| High availability | If you have BlackBerry UEM Cloud, instead of having to maintain your own highly available service for device management, with all the upfront and maintenance costs, BlackBerry maintains the service and maximizes uptime for you. |
| Migration | You can migrate users, devices, groups, and other data from an on-premises BlackBerry UEM source database to a new on-premises or BlackBerry UEM Cloud instance. |

| Feature | Description |
|---|---|
| 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). You can create a connection between Cisco ISE and BlackBerry UEM on-premises 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. |
| 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 who 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 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. |

# 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.<br>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:<br>• Lock the device, change the device or work space password, or delete information from the device<br>• Connect the device securely to your organization's mail environment, using Microsoft Exchange ActiveSync for email and calendar support<br>• Control how the device can connect to your organization's network, including Wi-Fi and VPN settings<br>• Configure single sign-on for the device so that it authenticates automatically with domains and web services in your organization's network<br>• Control the capabilities of the device, such as setting rules for password strength and disabling functions like the camera<br>• Manage app availability on the device, including specifying app versions and whether the apps are required or optional<br>• Search app stores directly for apps to assign to devices<br>• Install certificates on the device and optionally configure SCEP to permit automatic certificate enrollment<br>• 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.<br>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. |
| High availability and disaster recovery for the BlackBerry Infrastructure and BlackBerry UEM Cloud environments | BlackBerry data centers are located around the world and are designed to provide high availability and disaster recovery. BlackBerry data centers provide secure physical access to buildings, monitoring, and hardware redundancies to help protect your organization’s data from natural disasters.<br>BlackBerry data centers have disaster recovery plans for service outages. The plans are designed to have minimal impact on device users and ensure business continuity. Data and apps are backed up in near real time to avoid data loss. |
| 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. |

| Feature | Description |
|---|---|
| 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. |

# 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 | 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.<br>You can link multiple Apple DEP accounts to one BlackBerry UEM domain. |
| 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. |
| 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. |

| Feature | Description |
|---|---|
| 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.<br>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.<br>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 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. |
| IBM Notes Traveler support | iOS devices can 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. |
| 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:<br>• App lock mode enabled<br>• VPP apps assigned |

### Android devices

| Feature | Description |
|---|---|
| Manage Android Enterprise devices | You can activate Android devices 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.<br>Devices can be activated to have only a work profile, or to have both work and personal profiles. You can have full control over both profiles and have the ability to wipe the entire device, or you can allow user privacy for the personal profile and only have the ability to wipe work data from the device.<br>Samsung and BlackBerry powered by Android devices offer additional administrator options, including an enhanced set of IT policy rules, when activated with Android Enterprise |
| Work and personal – full control activations for Android Enterprise devices | This activation type is for devices running Android 8 and later. It lets you manage the entire device. It creates a work profile on the device that separates work and personal data but allows your organization to maintain full control over the device and wipe all data from the device. Data in both the work and personal profiles is protected using encryption and a method of authentication such as a password. |
| Manage devices using Knox MDM and Knox Workspace | BlackBerry UEM can also 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.<br>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:<br>• An enhanced set of IT policy rules<br>• Enhanced application management including silent app installations and uninstallations, silent uninstallations of restricted apps, and prohibitions to installing restricted apps<br>• App lock mode<br>For more information about supported devices, see the Compatibility matrix. For more information about Knox, visit https://www.samsungknox.com. |
| 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.<br>The profile allows you to enable BlackBerry Dynamics for users that are not already BlackBerry Dynamics enabled. |

| Feature | Description |
|---|---|
| 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 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 | Support for app-based PKI solutions, such as Purebred, which can enroll certificates for BlackBerry Dynamics apps. You can 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. |
| Security patch level enforcement for BlackBerry Dynamics apps | You can apply security patch level enforcement to BlackBerry Dynamics apps. If the security patch level is not met, you can choose to delete the BlackBerry Dynamics app data, not allow BlackBerry Dynamics apps to run on the device, or perform no actions on the device. |
| 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 Enterprise and Samsung Knox Workspace devices. |
| 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. |

#### Windows 10 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. |

| 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.<br>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. |
| Whitelist antivirus vendors | In the compliance profile, in the “Antivirus status” rule for Windows devices, you can choose to allow antivirus software from any vendor, or allow only those that you added to the “Allowed antivirus vendors” list. The rule will be enforced if a device has antivirus software enabled from any vendor that is not whitelisted. |
| Azure Active Directory Join | BlackBerry UEM supports Azure Active Directory Join which allows a simplified MDM enrollment process for Windows 10 devices. Users can enroll their devices with BlackBerry UEM using their Azure Active Directory username and password. Azure Active Directory Join is also required to support Windows AutoPilot, which allows Windows 10 devices to be automatically activated with BlackBerry UEM during the Windows 10 out-of-box setup experience. **Note**: To enable automatic MDM enrollment with BlackBerry UEM during the Windows 10 out-of-box setup, a BlackBerry UEM certificate must be installed on the device. |

### 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, in the BlackBerry UEM Compatibility Matrixes.

# Legal notice

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada