Overview and What's New Guide

BlackBerry UEM
Version 12.6

Published: 2016-12-22
SWD-20161222104350951

Contents

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 is BlackBerry UEM?

BlackBerry UEM is a multiplatform EMM solution from BlackBerry that provides comprehensive device, application, and content management with integrated security and connectivity.

With BlackBerry UEM you can:

- Manage BlackBerry 10, iOS, macOS, Android (including devices that use Android for Work and Samsung KNOX), Windows (including Windows 10 tablets and computers), and BlackBerry OS (version 5.0 to 7.1) devices
- Use a simple web-based interface to manage BYOD, COPE, and COBO devices and protect business information
- Manage complex fleets of devices using comprehensive reporting and dashboards, dynamic filters, and robust search capabilities
- Keep mobile workers connected with the information that they need
- Configure high availability to minimize service interruptions for device users
- Allow users to activate their own devices with BlackBerry UEM Self-Service
- Ensure data security across iOS, Android, Windows, and BlackBerry devices

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

BlackBerry Enterprise Mobility Suite services

Beyond the security and productivity features provided by BlackBerry UEM, BlackBerry offers more services that can add value to your BlackBerry UEM domain by meeting 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 macOS 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 your organization. • BlackBerry Enterprise Identity gives users single sign-on access to service providers such as BlackBerry Workspaces, Box, Workday, Cisco 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.

Service type	Service name and description
	• 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. • BlackBerry Notes allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their mobile device of choice.

What's new in BlackBerry UEM version 12.6

Branding

- **Product name**: BES12 is now BlackBerry UEM.

Android

- **Android for Work**: Enterprise deployment and user enrollment for Android for Work is simplified in BlackBerry UEM. To support Android for Work devices, you no longer need to set up a Google domain and connect it to BlackBerry UEM. You must have the most recent version of the BlackBerry UEM Client installed on your organization's devices before you can use this feature. The first version of the client that will be compatible with this feature will be available in January 2017.
- **Device logs**: You can send a "Get device logs" command from BlackBerry UEM for Android devices.

For more information about these features, see the Administration content.

iOS

- **iOS 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.
- **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 in BlackBerry UEM for supervised iOS devices running iOS 9.3 or later.
- **iOS Work Apps icon**: You can configure the iOS Work Apps icon so that users can view it in full screen mode on their devices.
- **iOS apps**: For supervised iOS 9.3.2 and later devices, you can specify a list of apps to allow on users' devices. All other apps can be installed but cannot be launched and will not be seen on devices. You can add any built-in apps directly to the allowed or restricted list in a compliance profile.
- **App configurations for iOS**: You can now create an app configuration from an XML template that uses the AppConfig schema, which is a standardized format defined by AppConfig Community, copy another app configuration, or create an app configuration manually.
- **Password autofill option for managed domains profiles**: Managed domains profiles include a new option to allow password autofill for the web domains that are specified in a profile. This option is supported for supervised iOS devices running iOS 9.3 or later.
- **Network usage profile**: When you configure the network usage profile, you now have the option to select apps from a list instead of typing the app package ID.

- **Wi-Fi profile — new QoS settings for iOS 10 devices**: For iOS 10 devices, you can configure QoS settings in Wi-Fi profiles to specify whether traffic can use L2 and L3 marking

For more information about these features, see the Administration content.

Device activation

- **Activate multiple devices**: You can let users activate multiple devices with different activation types by pairing activation passwords with activation profiles. For example, you might want users to activate work devices with a "full control" activation type and activate personal devices with an activation type that allows user privacy. You can now manually expire activation passwords at any time if required.
- **Device activation - certificate**: The device activation process for iOS and Android devices is streamlined. Users no longer need to verify and accept the certificate information to authenticate with BlackBerry UEM. This is now done automatically.

For more information about these features, see the Administration content.

Installation

- **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.

For more information about these features, see the Installation and upgrade content.

Management console

- **User list**: You can use Shift+click to select multiple users in the user list.

- **Rate and review apps**: You can specify whether users in your organization can rate and provide reviews of iOS, Android, and Windows 10 apps and see reviews provided by other users for internal custom apps or apps that are downloaded from public app storefronts. You must have the most recent version of the BlackBerry UEM Client installed on your organization's Android and Windows 10 devices before you can use this feature. The first version of the client that will be compatible with this feature will be available in January 2017.

- **Logging**: BlackBerry UEM can now generate log files where you can view phone call and SMS/MMS activity for Android for Work devices activated with “Work space only (Android for Work - Premium)” and Samsung KNOX Workspace devices activated with “Work and personal - full control (Samsung KNOX)” or “Work space only (Samsung KNOX)”. You must have the most recent version of the BlackBerry UEM Client installed on your organization's devices before you can use this feature. The first version of the client that will be compatible with this feature will be available in January of 2017.

- **Remove a Secure Work Space connection:** If you have an existing Secure Work Space connection, you can remove the connection and the menu item from the management console.
- **Restrict BlackBerry Secure Connect Plus to specific work space apps on Android for Work devices**: You can enable per-app VPN for Android for Work devices to restrict the use of BlackBerry Secure Connect Plus to specific work space apps that you add to an allowed list.

  For more information, see “Enable BlackBerry Secure Connect Plus” in the *Administration Guide*.

- **Additional options for Microsoft Active Directory connections**: When you specify key distribution center (KDC) domain controllers and global catalog servers, you can optionally include the port number that the domain controller uses (for example, kdc01.example.com:88). When you configure the Microsoft Active Directory account for each forest, you can also specify the KDC domain controllers and global catalog servers that you want BlackBerry UEM to use.
- **App deployment reports**: You can export app deployment reports to an .html file from the Apps screen in the management console. The report includes information about apps deployed by BlackBerry UEM and the users that have installed the apps on their devices.

For more information about these features, see the Administration content.

IBM Notes Traveler

- **IBM Notes Traveler support**: iOS devices can now connect to IBM Notes Traveler through BlackBerry Secure Gateway Service.

For more information about these features, see the Administration content.

BlackBerry Connectivity Node

- **The BlackBerry Connectivity Node now includes BlackBerry Proxy:** The BlackBerry Connectivity Node now includes the BlackBerry Proxy component. BlackBerry Proxy maintains a secure connection between your organization and the BlackBerry Dynamics NOC and also supports Direct Connect, which allows BlackBerry Dynamics app data to bypass the BlackBerry Dynamics NOC.

For more information about these features, see the Configuration content.

Ports

- **Updated port requirements:** BlackBerry UEM has new outbound port requirements to support connections to the BlackBerry Dynamics NOC, as well as new listening ports to support additional components like BlackBerry Control and BlackBerry Proxy. For more information, see the port requirements in the *Installation and Upgrade Guide*.

For more information about these features, see the Installation and upgrade content.

Monitoring

- **Monitoring**: You can monitor the status of the BlackBerry Cloud Connector using SNMP.

For more information about these features, see the Administration content.

Key BlackBerry UEM features

5

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 for Work, 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 for Work devices 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.
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.
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

Feature	Description
	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.

Key features for all device types

6

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

Feature	Description
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.
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.

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.
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

7

iOS devices

Feature	Description
Run app lock mode	On iOS devices that are supervised using Apple Configurator, 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. For more information about configuring BlackBerry UEM and activating iOS devices that are enrolled in the DEP, see the Configuration and the Administration content.
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 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 Good Dynamics profile to allow iOS devices to access BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. You

Feature	Description
	can assign the Good Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps. The Good Dynamics profile is added to the BlackBerry UEM management console when communication between BlackBerry UEM and the BlackBerry Control server is configured. The profile allows you to enable BlackBerry Dynamics for users that are not already Good 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.

Android devices

Feature	Description
Manage devices using Android MDM	Android MDM uses the basic management options that are native to the Android OS to manage the device. A separate, protected container is not created. For more information about managing devices using Android MDM, see the Administration content.
Manage devices using KNOX MDM and KNOX Workspace	BlackBerry UEM can manage Samsung devices using Samsung KNOX MDM and Samsung KNOX Workspace. KNOX Workspace provides an encrypted, password-protected container on a Samsung device that includes your work apps and data. It separates a user's personal apps and data from your organization's apps and data and protects your apps and data using enhanced security and management capabilities that Samsung developed.

Feature	Description
	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 using Android for Work	You can activate Android devices that run Android OS 5.1 or later to use Android for Work. Android for Work is a feature developed by Google that provides additional security for organizations that want to manage Android devices and allow their data and apps on Android devices. For more information about managing devices using Android for Work, see the Administration content.
Integration with BlackBerry Dynamics	You can use the Good 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 Good Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps. The Good Dynamics profile is added to the BlackBerry UEM management console when communication between BlackBerry UEM and the BlackBerry Control server is configured. The profile allows you to enable BlackBerry Dynamics for users that are not already Good enabled.
Per-app VPN	You can enable per-app VPN for Android for Work devices 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.
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.

Feature	Description
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.

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

8

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 Android for Work 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	- BlackBerry PlayBook - 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

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 for Work 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, BES12 Cloud, Strong Authentication by BlackBerry, Enterprise Identity by BlackBerry, and WatchDox by BlackBerry

Glossary

10

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

11

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

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

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING

OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

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

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

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

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

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

BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

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

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

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada