BlackBerry UEM

Overview and Architecture

12.20

Contents

What is BlackBerry UEM?

BlackBerry UEM is a multiplatform EMM solution that provides comprehensive device, app, and content management with integrated security and connectivity, and helps you manage iOS, macOS, Android, and Windows devices for your organization.

You can install UEM in an on-premises environment for maximum control over your servers, data, and devices, or you can use UEM Cloud, which offers an easy-to-use, low-cost, and secure solution. BlackBerry hosts UEM Cloud over the Internet, so you only need a supported web browser to access the service.

Both UEM on-premises and UEM Cloud offer trusted end-to-end security and provide the control that organizations need to manage all endpoints and ownership models.

The benefits of UEM include:

Feature	Benefit
Low total cost of ownership	UEM on-premises reduces complexity, optimizes pooled resources, ensures maximum uptime, and helps you achieve the lowest total cost of ownership for an on-premises solution. UEM Cloud reduces the cost of ownership by removing the need to install, manage, and update services.
Single web-based interface	Manage iOS, macOS, Android, and Windows devices, plus additional services, 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 on UEM 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 on-premises to minimize service interruptions for device users or rely on BlackBerry to maintain UEM Cloud and maximize uptime for you.
Additional services available	Enable services such as BlackBerry Workspaces, BlackBerry Enterprise Identity, BlackBerry 2FA, BBM Enterprise, and UEM Notifications to add value to your UEM deployment.

Key BlackBerry UEM features

Feature	Description
Multiplatform device management	You can manage iOS, macOS, Android, and Windows 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 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 data.
Separate work and personal needs	You can manage devices using Android Enterprise, Android Management, and Samsung Knox technologies that are designed to keep personal and work information separate and secure on devices. If a device is lost or compromised, 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 iOS 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 ensuring 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 UEM Self-Service, users can activate or switch devices, change their device password remotely, delete device data, or lock a lost or stolen device.
Integration with other BlackBerry services	You can integrate UEM with BlackBerry Workspaces, BlackBerry Enterprise Identity, and BlackBerry 2FA to add value to your organization's UEM instance.
Powerful app management	UEM is a comprehensive app management platform for all devices. You can deploy apps from all major app stores, including the App Store and Google Play.
Role-based administration	You can share duties with multiple administrators who can access the management console at the same time. You can use roles to define the actions that an administrator can perform, allowing you to reduce security risks, distribute job responsibilities, and increase efficiency. You can use predefined roles or create your own custom roles.

Feature	Description
Company directory integration	You can use local, built-in user authentication to access the management console and self-service console, or you can integrate UEM with Microsoft Active Directory, LDAP, or Entra ID directories that you use in your organization's environment. UEM supports connections to multiple directories. You can create user accounts in UEM using user data from the directory, and you can link company directory groups with UEM to organize users in UEM the same way that they are organized in your company directory. You can also enable onboarding for specific groups in your company directory to create UEM users automatically. If you enable onboarding, you can also configure offboarding to delete device data or user accounts when users are removed from groups in your company directory.
Migration	You can migrate users, devices, groups, and other data from an on-premises UEM source database to a new on-premises or UEM Cloud instance.
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 UEM on-premises so that Cisco ISE can retrieve data about the devices that are activated on 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 wearable devices in 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 UEM management capabilities that are supported include device activation using a QR code, IT policies, Wi-Fi and VPN profiles, app management, and location services.

Feature	Description
Microsoft Intune integration	For iOS and Android devices, if you want to protect data in Microsoft 365 apps using the MAM features of Microsoft Intune, you can use Intune to protect app data while using 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

Feature	Description
Activate devices	When a user activates a device, they associate it with UEM and your organization's environment so that they can access work data on the device. Users can activate their devices using a QR code or their email address and an activation password. You can allow users to activate devices themselves or you can activate devices for users and then distribute them. All device types can be activated over the wireless network.
Manage devices	You can view all devices and access all management tasks in a single, web-based console. You can manage multiple devices for each user account and view the device inventory for your organization. You can perform the following actions if they 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 apps are required or optional. • Search app stores directly for apps to assign to devices. • Install certificates on the device and optionally configure SCEP to permit automatic certificate enrollment. • Extend email security using S/MIME or PGP.
Manage groups of users, apps, and devices	Groups simplify the management of users, apps, and devices. You can use groups to apply the same configuration settings to similar user accounts or similar devices. You can assign different groups of apps to different groups of users, and a user can be a member of several groups.

Feature	Description
Control which devices can access Microsoft Exchange ActiveSync	You can use gatekeeping to ensure that only devices managed by 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 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 device requirements	You can use a compliance profile to help enforce your organization's security requirements, 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.
Create or import many user accounts with a .csv file	You can import a .csv file into 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 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	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. 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
Device activation	You can use Apple Configurator 2 to prepare devices for activation with UEM. Users can activate the prepared devices without using the BlackBerry UEM Client.
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 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 UEM domain so that you can distribute purchased licenses for iOS apps associated with the VPP accounts.
Apple Device Enrollment Program	You can configure UEM to use the Apple Device Enrollment Program (DEP) so that you can synchronize UEM with the DEP. After you configure UEM, you can use the management console to manage the activation of the iOS devices that your organization purchased for the DEP. You can use multiple DEP accounts. You can link multiple Apple DEP accounts to one UEM domain.
Support for app-based PKI solutions	UEM supports 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.
Custom payload profiles	You can use custom payload profiles to control features on iOS devices that are not controlled by existing UEM policies or profiles. You can create Apple configuration profiles using Apple Configurator and add them to UEM custom payload profiles. You can assign the custom payload profiles to users, user groups, and device groups.
BlackBerry Secure Gateway	BlackBerry Secure Gateway allows iOS devices with the MDM controls activation type to connect to your work email server through the BlackBerry Infrastructure and UEM. If you use 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. 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 web pages 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 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.
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.
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	UEM supports Face ID for device authentication and to open BlackBerry Dynamics apps.

Feature	Description
Shared device management	You can allow multiple users to share an iOS device. You can customize terms of use that users must accept to check out shared devices. A user can check out a device using local authentication and when they are done using it, they can check it in and the device is available for the next user. Shared devices remain managed by UEM during the check-out and check-in process. This feature was designed for supervised devices with the following configuration: • App lock mode enabled • VPP apps assigned
iPad	iPad devices can be shared between multiple users. When users sign in with a managed Apple ID, their data loads and the user can access their own email accounts, files, iCloud photo library, app data, and more.

Android devices

Feature	Description
Manage Android Enterprise and Android Management devices	You can activate Android devices to use Android Enterprise or Android Management, which are features developed by Google that provide additional security for organizations that want to manage and allow apps and data on Android devices. 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. Samsung 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 and Android Management devices	This activation type allows you to 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.

Feature	Description
Manage devices using Knox MDM and Knox Workspace	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 work apps and data using enhanced security and management capabilities that Samsung developed. When a device is activated, UEM automatically identifies whether the device supports Knox. In addition to the standard Android management capabilities, UEM includes the following 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.
Integration with BlackBerry Dynamics	You can use the BlackBerry Dynamics profile to allow Android devices to access BlackBerry Dynamics productivity apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect. You can assign the BlackBerry Dynamics profile to user accounts, user groups, or device groups. Multiple devices can access the same apps. The profile allows you to enable BlackBerry Dynamics for users that are not already BlackBerry Dynamics enabled.
Per-app VPN	You can enable per-app VPN for Android devices that have a work profile to restrict the use of BlackBerry Secure Connect Plus to specific work space apps that you add to an allowed list.
Zero-touch enrollment	UEM supports devices 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. Zero-touch enrollment makes it simple for IT administrators to configure devices online and have enforced management ready when employees receive their devices. For more information from Google, see Zero-touch enrollment management and the zero-touch enrollment overview. 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	UEM supports 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.

Feature	Description
SafetyNet and Play Integrity	When administrators enable Android SafetyNet or Google Play Integrity attestation, 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 devices

Feature	Description
Support for Windows 10 devices	You can manage Windows devices, including Windows 10 Mobile devices and Windows 10 tablets and computers.
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 web pages 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.
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 of your organization, and audit inappropriate data sharing practices. You can specify which apps are protected and trusted to create and access work files.
Allow 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 allowed.

Feature	Description
Entra ID Join	UEM supports Entra ID Join, which allows a simplified MDM enrollment process for Windows 10 devices. Users can enroll their devices with UEM using their Entra ID username and password. Entra ID 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.

macOS devices

Feature	Description
Basic device management using device controls	When a user activates a macOS device, the device and the user are set up as separate entities on UEM. Separate communication channels are established between UEM and the device and UEM and the user account, allowing you to manage the device and the user separately.
Profiles and policies	Some profiles are assigned to the user only (for example, email profiles). Some profiles are assigned to the device only (for example, proxy profiles). Some profiles allow you to choose whether to apply the profile to the device or the user (for example, Wi-Fi profiles). You can control the device using commands and IT policies. Users activate macOS devices using BlackBerry UEM Self-Service.

Supported features by device type

This quick reference compares the supported capabilities of iOS, macOS, Android, and Windows 10 devices in BlackBerry UEM.

For more information about supported OS versions, see the Compatibility matrix.

Device features

Feature	iOS	macOS	Android	Windows 10
Wireless activation	√	√	√	√
Wireless activation using a QR code	√		√	
Client app required for activation	√ [1]		√	
Customize terms of use agreement for activation	√	√	√	√
Restrict activation by device model	√	√	√	

Feature	iOS	macOS	Android	Windows 10
View and export device report (e.g., hardware details)	√	√	√	√
Restrict unsupervised devices	√[2]	√[2]		

[1] For iOS devices enrolled in DEP, client app must be assigned to users or groups.

[2] For devices activated with MDM controls, or User privacy with SIM-based licensing only.

Security features

Feature	iOS	macOS	Android	Windows 10
Separation of work and personal data	√ [1]		√ [2]	√
User privacy for personal data	√ [1]		√ [2]	
Encryption of work data at rest	√ [1]		√ [2]	√
Send IT commands to devices	√	√	√	√
Control device capabilities using IT policies	√	√	√	√
Delete work data after period of inactivity	√ [1]		√ [1]	
Enforce password requirements	√	√	√	√
Enforce encryption of media card			√ [3]	
Enforce encryption of internal storage			√	√

[1] Requires BlackBerry Dynamics apps.

[2] Requires Samsung Knox Workspace, Android Enterprise, Android Management, or BlackBerry Dynamics apps.

[3] For Samsung Knox devices only.

Sending certificates to devices

Feature	iOS	macOS	Android	Windows 10
CA certificate profiles	√	√	√	√
SCEP profiles	√	√	√	√

Feature	iOS	macOS	Android	Windows 10
Shared certificate profiles	√	√	√	
User credential profiles	√	√	√	

Managing work connections for devices

Feature	iOS	macOS	Android	Windows 10
BlackBerry 2FA profiles	√		√	
BlackBerry Dynamics connectivity profiles	√	√	√	√
CalDAV profiles	√	√		
CardDAV profiles	√	√		
Enterprise connectivity				
BlackBerry Secure Connect Plus	√		√ [1]	
Exchange ActiveSync email profiles	√	√	√ [2]	√
BlackBerry Secure Gateway	√			
IMAP/POP3 email profiles	√	√	√	√
Proxy profiles	√	√	√	√
Single sign-on profiles	√			
VPN profiles	√	√	√ [3]	√
Wi-Fi profiles	√	√	√	√

[1] Only for Android Enterprise devices and Knox Workspace devices.

[2] Only for Motorola devices that support the EDM API, Android Enterprise devices, and Knox devices.

[3] For Knox Workspace devices only.

Managing your organization's standards for devices

Feature	iOS	macOS	Android	Windows 10
Activation profiles	√	√	√	√

Feature	iOS	macOS	Android	Windows 10
App lock mode profiles	√ [1]		√ [1]	√ [1]
BlackBerry Dynamics profiles	√	√	√	√
Compliance profiles	√		√	
Device profiles	√		√	
Enterprise Management Agent profiles	√		√	√
Location service profiles	√		√	√

[1] Only for supervised iOS devices, Knox devices that are activated with MDM controls, Windows 10 Education, and Windows 10 Enterprise devices.

Protecting lost or stolen devices

Feature	iOS	macOS	Android	Windows 10
Specify device password			√	
Lock device	√	√	√	
Activation lock	√			
Specify device password and lock			√	
Specify work space password and lock			√ [1]	
Unlock device and clear password	√		√	
Delete all device data	√	√	√ [2]	√
Delete only work data	√	√	√	√

[1] Only for Android Enterprise devices.

[2] For Motorola devices that support the EDM API, information on the media card is also deleted. For Knox Workspace devices, you can choose to delete information on the media card.

Configuring roaming

Feature	iOS	macOS	Android	Windows 10
Disable automatic synchronization when roaming	√		√ [1]	

Feature	iOS	macOS	Android	Windows 10
Disable data when roaming	√[2]		√ [3]	√

[1] For Knox devices only.

[2] You can configure data roaming settings in a network usage profile.

[3] For Android Enterprise and Knox devices only.

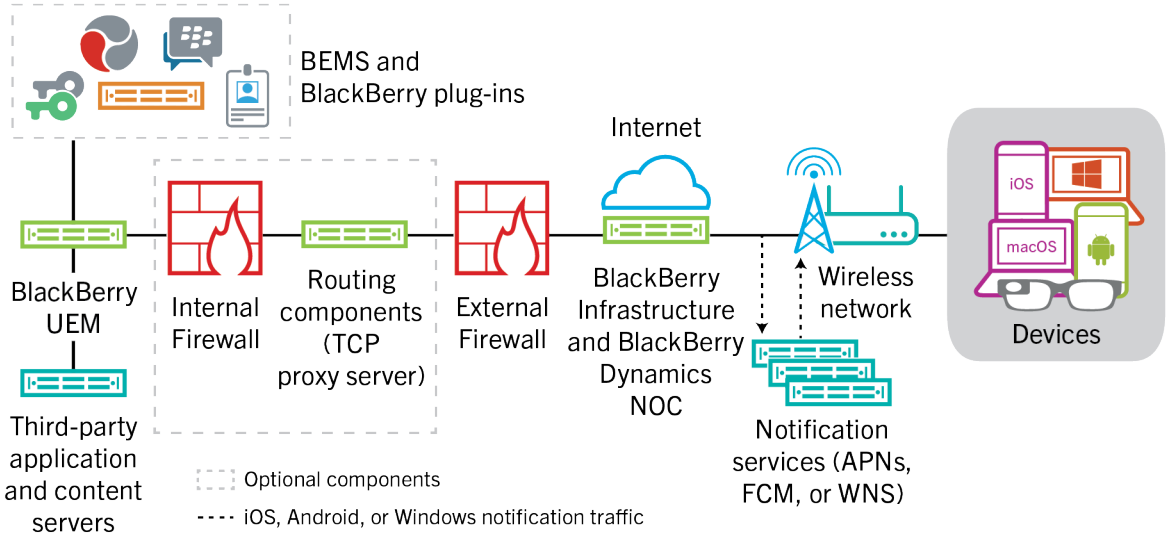
Managing apps

Feature	iOS	macOS	Android	Windows 10
Distribute public apps from storefront (App Store, Google Play, Windows Store, BlackBerry World)	√		√	√
Manage work app catalog	√		√	√
Brand work app catalog	√			
Restrict apps	√		√	
Distribute internal apps	√		√	√
Add app shortcuts to devices	√	√	√	

BlackBerry UEM architecture

The BlackBerry UEM architecture is designed to help you manage mobile devices for your organization and provide a secure link for data to travel between your organization's mail and content servers and your user's devices.

Architecture: BlackBerry UEM solution

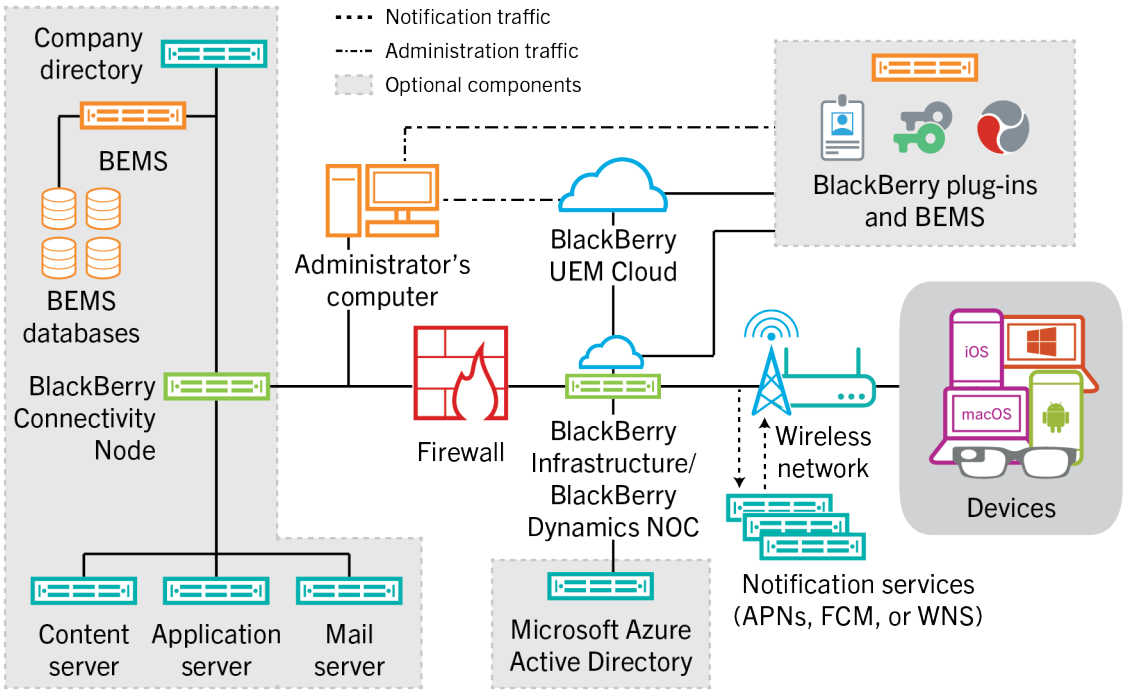


Component	Description
BlackBerry UEM	BlackBerry UEM is a unified endpoint management solution that provides comprehensive multiplatform device, application, and content management with integrated security and connectivity.
BlackBerry Infrastructure	The BlackBerry Infrastructure is a global private data network distributed across multiple regions that enables and secures data in transit between thousands of organizations and millions of users around the world. It is designed to efficiently manage the transport of data between BlackBerry services and end-user devices. For organizations using UEM, the BlackBerry Infrastructure registers user information for device activation, validates licensing information, and provides a trusted path between the organization and every user based on strong cryptographic mutual authentication. UEM maintains a constant connection to the BlackBerry Infrastructure, ensuring that organizations require only a single outbound connection to a trusted IP address to send data to users. All the data that travels between the BlackBerry Infrastructure and UEM is authenticated and encrypted to provide a secure communication channel into your organization for devices outside the firewall.
BlackBerry Dynamics NOC	The BlackBerry Dynamics NOC is a network operations center that provides secure communications between BlackBerry Dynamics apps on devices, UEM, and the BlackBerry Enterprise Mobility Server.

Component	Description
Devices	BlackBerry UEM supports iOS, macOS, Android, and Windows devices.
Notification services	UEM sends notifications to devices to contact UEM for updates and to report information for your organization's device inventory. These notifications are sent to the BlackBerry Infrastructure, where they are sent to the devices using the appropriate notification service: • APNs is a service that Apple provides to send notifications to iOS and macOS devices. • FCM is a service that Google provides to send notifications to Android devices. • Windows Push Notification Services (WNS) is a service that Microsoft provides to send notifications to Windows devices.
Routing components	By default, UEM makes a direct connection to the BlackBerry Infrastructure over ports 3101 and 443, and you do not need to install more routing components. If your organization's security standards require that internal systems cannot make connections directly to the Internet, you can use the BlackBerry Router or a proxy server. The BlackBerry Router acts as a proxy server for connections over the BlackBerry Infrastructure between UEM and all devices. The BlackBerry Router can support SOCKs v5 with no authentication. If your organization already has a TCP proxy server installed, or needs one to meet networking requirements, you can use a TCP proxy server instead of the BlackBerry Router. The TCP proxy server can support SOCKs v5 with no authentication. The BlackBerry UEM Core and BlackBerry Proxy support using an HTTP proxy server to connect to the BlackBerry Dynamics NOC.
Third-party application and content servers	Additional content servers and application servers in your organization's environment, including the company directory, mail server, certificate authorities, and so on.
BlackBerry plug-ins and BEMS	UEM works with additional BlackBerry enterprise products such as BlackBerry Enterprise Identity, BlackBerry 2FA, and BlackBerry Workspaces to extend UEM capabilities in your organization. For more information, see Companion products and services. The BlackBerry Enterprise Mobility Server provides services to send work data to and from BlackBerry Dynamics apps. For more information, see the BlackBerry Enterprise Mobility Server docs.

Architecture: BlackBerry UEM Cloud solution

The BlackBerry UEM Cloud architecture was designed to help you manage mobile devices for your organization in a cloud environment and provide a secure link for data to travel between your organization's mail and content servers and your users' devices.



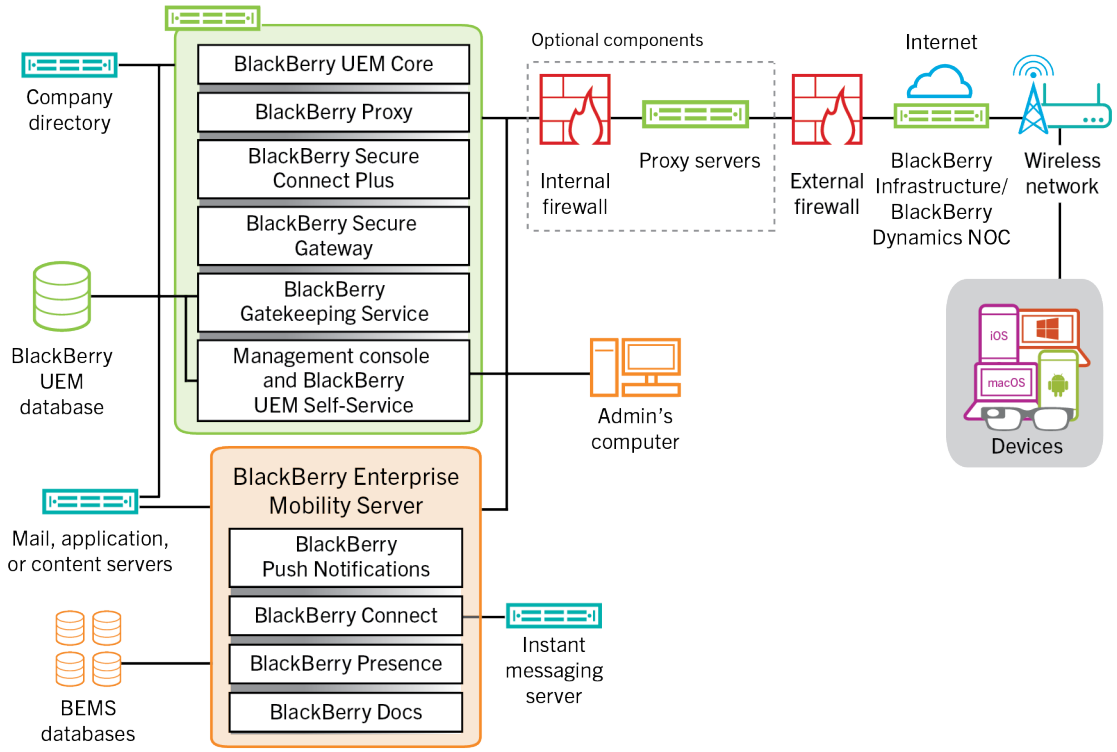
Component	Description
BlackBerry UEM Cloud	BlackBerry UEM Cloud is a service that allows you to manage devices used in your organization's environment.
BlackBerry Infrastructure and BlackBerry Dynamics NOC	The BlackBerry Infrastructure registers user information for device activation and validates licensing information. If you enable BlackBerry Secure Connect Plus or the BlackBerry Secure Gateway, data in transit that uses these services passes through the BlackBerry Infrastructure. The BlackBerry Dynamics NOC is a separately located NOC that provides secure communications between BlackBerry Dynamics apps on devices and BlackBerry Proxy installed behind the firewall as part of the BlackBerry Connectivity Node.
Devices	BlackBerry UEM Cloud supports iOS, macOS, Android, and Windows devices.
Notification services	UEM Cloud sends notifications to devices to contact UEM for updates and to report information for your organization's device inventory. These notifications are sent to the BlackBerry Infrastructure, where they are sent to devices using the appropriate notification service: • APNs is a service that Apple provides to send notifications to iOS and macOS devices. • FCM is a service that Google provides to send notifications to Android devices. • WNS is a service that Microsoft provides to send notifications to Windows 10 devices.

Component	Description
BlackBerry Connectivity Node	The BlackBerry Connectivity Node is an optional component that you install inside your organization's firewall. It includes the following components that add functionality to UEM Cloud: • The BlackBerry Cloud Connector connects UEM Cloud to your company directory behind the firewall to allow basic attribute synchronization, search functionality, and user authentication services. If you don't install the BlackBerry Connectivity Node and your company directory is behind the firewall, you must create local user accounts in UEM Cloud instead of using the user accounts in your company directory. The BlackBerry Cloud Connector is not required for UEM Cloud to connect to Microsoft Entra ID. • BlackBerry Proxy maintains a secure connection between your organization and the BlackBerry Dynamics NOC, which allows BlackBerry Dynamics apps to communicate securely with your organization's resources behind the firewall. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC. • The BlackBerry Gatekeeping Service sends commands to Exchange ActiveSync to add devices to an allowed list when devices are activated on UEM Cloud. Unmanaged devices that try to connect to an organization's mail server can be reviewed, verified, and blocked or allowed by an administrator using the UEM management console. • BlackBerry Secure Connect Plus provides a secure IP tunnel between work apps on devices and your organization's network. One tunnel that supports standard IPv4 (TCP and UDP) data is established for each device through the BlackBerry Infrastructure. • BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and UEM Cloud to your organization's mail server for iOS devices.
Company directory	UEM Cloud supports connectivity with your organization's Microsoft Active Directory or LDAP company directory behind the firewall using the BlackBerry Connectivity Node.
Microsoft Entra ID (formerly Azure AD)	Microsoft Entra ID is a cloud-based directory management service. If your organization uses Entra ID, you can connect to it instead of, or in addition to, a company directory behind the firewall.
Content, application, and mail servers	When you enable BlackBerry Secure Connect Plus or when users have BlackBerry Dynamics apps, devices can connect to your organization's servers without requiring you to open a direct connection between the server and the Internet. Work data in transit between your servers and devices is sent through BlackBerry Secure Connect Plus and the BlackBerry Infrastructure. BlackBerry Dynamics app data is sent through BlackBerry Proxy and the BlackBerry Dynamics NOC. BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and BlackBerry Connectivity Node between your organization's mail server and iOS devices.

Component	Description
BlackBerry plug-ins and BEMS	UEM works with additional BlackBerry enterprise products such as BlackBerry Enterprise Identity, BlackBerry 2FA, and BlackBerry Workspaces to extend UEM capabilities in your organization. For more information, see Companion products and services. The BlackBerry Enterprise Mobility Server provides services to send work data to and from BlackBerry Dynamics apps. For more information, see the BlackBerry Enterprise Mobility Server docs.

BlackBerry UEM on-premises components

This diagram shows how the BlackBerry UEM components connect when all components are installed together in the product's simplest configuration.



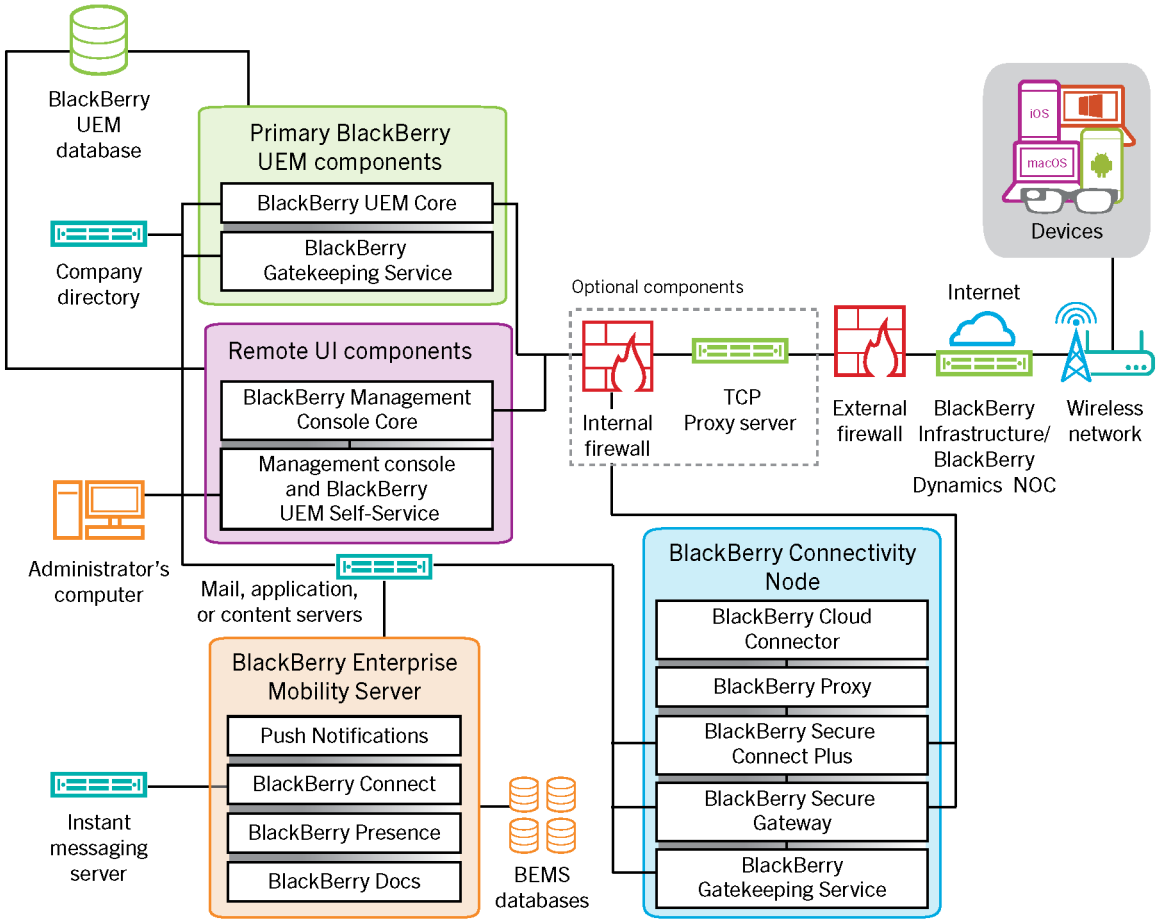
Component name	Description
BlackBerry UEM Core	The BlackBerry UEM Core is the central component of the UEM architecture. It consists of several subcomponents that are responsible for: • Logging, monitoring, reporting, and management functions • Authentication and authorization services • Scheduling and sending commands, IT policies, and profiles to devices • Sending user, policy, and other configuration data to BlackBerry Dynamics apps.
BlackBerry Proxy	BlackBerry Proxy maintains a secure connection between your organization and the BlackBerry Dynamics NOC. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus provides a secure IP tunnel between work apps on devices and your organization's network. One tunnel that supports standard IPv4 (TCP and UDP) data is established for each device through the BlackBerry Infrastructure.

Component name	Description
BlackBerry Secure Gateway	The BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and UEM to your organization's mail server for iOS devices.
BlackBerry Gatekeeping Service	The BlackBerry Gatekeeping Service sends commands to Exchange ActiveSync to add devices to an allowed list when devices are activated on UEM. Unmanaged devices that try to connect to an organization's mail server can be reviewed, verified, and blocked, or allowed by an administrator using the management console.
Management console and BlackBerry UEM Self-Service	The management console and BlackBerry UEM Self-Service provide a web-based user interface for administrator and user access to UEM. You use the management console to manage system settings, users, devices, and apps. Users can use UEM Self-Service to set an activation password and send commands to devices, such as set password, lock device, and delete device data.
BlackBerry UEM database	The UEM database is a relational database that contains user account information and configuration information that UEM uses to manage devices and BlackBerry Dynamics apps.
BlackBerry Enterprise Mobility Server	BEMS consolidates several services used to send work data to and from BlackBerry Dynamics apps, including: • BlackBerry Push Notifications: Accepts push registration requests from iOS and Android devices and then communicates with Microsoft Exchange to monitor the user's work mail account for changes. • BlackBerry Connect: Provides secure instant messaging, company directory look-up, and user presence information to iOS and Android devices. • BlackBerry Presence: Provides real-time presence status to BlackBerry Dynamics apps. • BlackBerry Docs: Allows your BlackBerry Dynamics app users to access, synchronize, and share documents using their work file server, SharePoint, Box, and content management systems supporting CMIS, without the need for VPN software, firewall reconfiguration, or duplicate data stores. The BEMS databases store user, app, policy, and configuration information.
BlackBerry Router and/or proxy servers	By default, UEM makes a direct connection to the BlackBerry Infrastructure over ports 3101 and 443. If your organization's security standards require that internal systems not connect directly to the Internet, you can install the BlackBerry Router or use a third-party TCP proxy server that supports SOCKs v5 with no authentication. The UEM Core and BlackBerry Proxy support using a third-party HTTP proxy server to connect to the BlackBerry Dynamics NOC.

Component name	Description
BlackBerry Infrastructure and BlackBerry Dynamics NOC	The BlackBerry Infrastructure registers user information for device activation, validates licensing information, and provides a trusted path between the organization and every user based on strong cryptographic mutual authentication. The BlackBerry Dynamics NOC is a separately-located NOC that provides secure communications between BlackBerry Dynamics apps on devices and the UEM Core, BlackBerry Proxy, and BEMS.

BlackBerry UEM on-premises distributed installation

This diagram shows how the BlackBerry UEM components connect together when the BlackBerry Connectivity Node and the user interface are both installed separately from the primary UEM components.



Component name	Description
Primary UEM components	The primary UEM components include the BlackBerry UEM Core and all components installed with it on the same server.
BlackBerry UEM Core	The UEM Core is the central component of the UEM architecture. It consists of several subcomponents that are responsible for: • Logging, monitoring, reporting, and management functions • Authentication and authorization services • Scheduling and sending commands, IT policies, and profiles to devices • Sending user, policy, and other configuration data to BlackBerry Dynamics apps on devices.

Component name	Description
BlackBerry UEM database	The UEM database is a relational database that contains user account information and configuration information that UEM uses to manage devices and BlackBerry Dynamics apps.
BlackBerry Gatekeeping Service (primary)	The BlackBerry Gatekeeping Service sends commands to Exchange ActiveSync to add devices to an allowed list when devices are activated on UEM. Unmanaged devices that try to connect to an organization's mail server can be reviewed, verified, and blocked or allowed through the management console.
Remote UI components	The management console and BlackBerry UEM Self-Service can be installed separately from other UEM components. If you install them separately, an instance of the BlackBerry Management Console Core is also installed.
BlackBerry Management Console Core	If installed, the BlackBerry Management Console Core processes only UI requests from the management console and UEM Self-Service. This ensures that these interfaces are responsive even when the load on the UEM Core is high.
Management console and BlackBerry UEM Self-Service	The management console and UEM Self-Service provide a web-based user interface for administrator and user access to UEM. It can be installed separately from other components. You use the management console to manage system settings, users, devices, and apps. Users can access UEM Self-Service to set an activation password and send commands, such as set password, lock device, and delete device data, to devices.
BlackBerry Connectivity Node	The BlackBerry Connectivity Node installs instances of the UEM device connectivity components in your organization’s domain on a different server than the UEM Core. Each BlackBerry Connectivity Node contains these components: • BlackBerry Cloud Connector: Allows the BlackBerry Connectivity Node components to communicate with the UEM Core. All communication between the BlackBerry Cloud Connector and the UEM Core travels through the BlackBerry Infrastructure. • BlackBerry Proxy: Maintains the secure connection between your organization and the BlackBerry Dynamics NOC. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC. • BlackBerry Secure Connect Plus: Provides a secure IP tunnel between work apps on devices and your organization's network. One tunnel that supports standard IPv4 (TCP and UDP) data is established for each device through the BlackBerry Infrastructure. • BlackBerry Secure Gateway: Provides a secure connection through the BlackBerry Infrastructure and UEM to your organization's mail server for iOS devices. • BlackBerry Gatekeeping Service: Manage gatekeeping for your mail server. If you want gatekeeping data to be managed only by the BlackBerry Gatekeeping Service that is installed with the primary UEM components, you can disable the BlackBerry Gatekeeping Service in each BlackBerry Connectivity Node.

Component name	Description
BlackBerry Enterprise Mobility Server	BEMS consolidates several services used to send work data to and from BlackBerry Dynamics apps, including: • BlackBerry Push Notifications: Accepts push registration requests from iOS and Android devices and then communicates with Microsoft Exchange to monitor the user's work mail account for changes. • BlackBerry Connect: Provides secure instant messaging, company directory look-up, and user presence information to iOS and Android devices. • BlackBerry Presence: Provides real-time presence status to BlackBerry Dynamics apps. • BlackBerry Docs: Allows your BlackBerry Dynamics app users to access, synchronize, and share documents using their work file server, SharePoint, Box, and content management systems supporting CMIS, without the need for VPN software, firewall reconfiguration, or duplicate data stores. The BEMS databases store user, app, policy, and configuration information.
BlackBerry Infrastructure and BlackBerry Dynamics NOC	The BlackBerry Infrastructure registers user information for device activation, validates licensing information, and provides a trusted path between the organization and every user based on strong cryptographic mutual authentication. The BlackBerry Dynamics NOC is a separately-located NOC that provides secure communications between BlackBerry Dynamics apps on devices and the UEM Core, BlackBerry Proxy, and BEMS.

Companion products and services

This section provides information about the many companion products and services that can be used with BlackBerry UEM.

Enterprise and BlackBerry Dynamics apps

BlackBerry 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 UEM to manage iOS and Android devices. Users require the UEM Client to activate iOS or Android devices for mobile device management with UEM. Users can download the latest version of the UEM Client from the App Store or Google Play. After users activate their devices, the UEM Client allows users to do the following: • Verify whether their devices are compliant with the organization's standards • View the profiles that have been assigned to them • View the IT policy rules that have been assigned to them • Access work apps • Create access keys for BlackBerry Dynamics apps • Preauthenticate with BlackBerry 2FA • Access a software OTP code • Retrieve and email device log files • Deactivate their devices For more information, see the UEM Client docs.
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, Windows, and macOS devices. BBM Enterprise uses a FIPS 140-2 validated cryptographic library. Your organization owns the encryption keys and no one else, not even BlackBerry, can access them. For most devices, you can use UEM to assign BBM Enterprise to users. After you enable users to use BBM Enterprise, users can download the app from the appropriate app store. For more information, see the BBM Enterprise docs.

BlackBerry Dynamics apps

BlackBerry Dynamics productivity apps provide users with access to work data and productivity tools.

App	Description
BlackBerry Work	The BlackBerry Work app provides secure access to work email and allows users to view and send attachments, create custom contact notifications, and manage their messages. For more information, see the BlackBerry Work docs.
BlackBerry Access	BlackBerry Access is a secure browser that allows users to access work intranets and web applications. BlackBerry Access also allows you to enable access to work resources or build and deploy rich HTML5 apps, while maintaining a high level of security and compliance. For more information, see the BlackBerry Access docs.
BlackBerry Connect	BlackBerry Connect allows communication and collaboration with secure instant messaging, company directory lookup, and user presence from an easy-to-use interface on the user's device. For more information, see the BlackBery Connect docs.
BlackBerry Tasks	BlackBerry Tasks allows users to create, edit, and manage tasks that are synchronized with Microsoft Exchange. For more information, see the BlackBerry Tasks docs.
BlackBerry Notes	BlackBerry Notes allows users to create, edit, and manage notes that are synchronized with Microsoft Exchange on their mobile device of choice. For more information, see the BlackBerry Notes docs.
BlackBerry BRIDGE	BlackBerry BRIDGE is a Microsoft Intune app that is enabled for BlackBerry Dynamics. It allows you to securely view, edit, and save documents using Intune-managed Microsoft apps, such as Microsoft Word, Microsoft PowerPoint, and Microsoft Excel in BlackBerry Dynamics on iOS and Android devices. For more information, see the BlackBerry Bridge docs.

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.

Your organization can also develop custom BlackBerry Dynamics apps using the BlackBerry Dynamics SDK. For more information, see the BlackBerry Dynamics SDK docs.

Benefits of BlackBerry Enterprise Identity

BlackBerry Enterprise Identity makes it easy for users to access cloud applications from any device, including iOS, Android, and 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 365, Google Workspace, 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 UEM management console to add services, manage users, and to add and manage additional administrators. The integration with UEM makes it easy to manage users and entitle them to access cloud applications and services from their devices. Cloud services and mobile app binaries can be bundled together and then simply assigned to users and groups.

For more information, see the BlackBerry Enterprise Identity docs.

Benefits of BlackBerry 2FA

BlackBerry 2FA provides users with two-factor authentication to access your organization's resources. It allows you to use iOS and Android devices as the second factor of authentication through a simple confirmation prompt when users try to connect to your organization's 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 UEM 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.

For more information, see the BlackBerry 2FA docs.

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 that 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 iOS and Android 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 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, see the BlackBerry Workspaces docs.

Benefits of BlackBerry UEM Notifications

BlackBerry UEM Notifications takes advantage of the BlackBerry AtHoc Networked Crisis Communication system to allow administrators to 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 is available for use with BlackBerry UEM on-premises only.

For more information, see the UEM Notifications docs.

BlackBerry enterprise SDKs

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

SDK	Description
BlackBerry Dynamics SDK	The BlackBerry Dynamics SDK provides a powerful set of tools that allow developers to focus on building useful productivity apps rather than learning how to secure, deploy, and manage those apps. Developers can use the BlackBerry Dynamics SDK to develop apps for all major platforms that leverage valuable services, including secure communications, interapp data exchange, presence, push, directory lookup, single sign-on authentication, and identity and access management. For more information, see the BlackBerry Dynamics SDK docs.
BlackBerry Web Services	The BlackBerry Web Services are a collection of SOAP and REST web services that developers can use to create applications to manage your organization's UEM domain, user accounts, and all supported devices. You can use the BlackBerry Web Services to automate many tasks that administrators typically perform using the management console. For example, you can create an application that automates the process of creating user accounts, adds users to multiple groups, and manages users' devices. For more information, see the BlackBerry Web Services docs.
BlackBerry Workspaces Android SDK	Developers can use the BlackBerry Workspaces Android SDK to develop apps to enable users to work with files protected by BlackBerry Workspaces. For more information, see the BlackBerry Workspaces Android SDK docs.

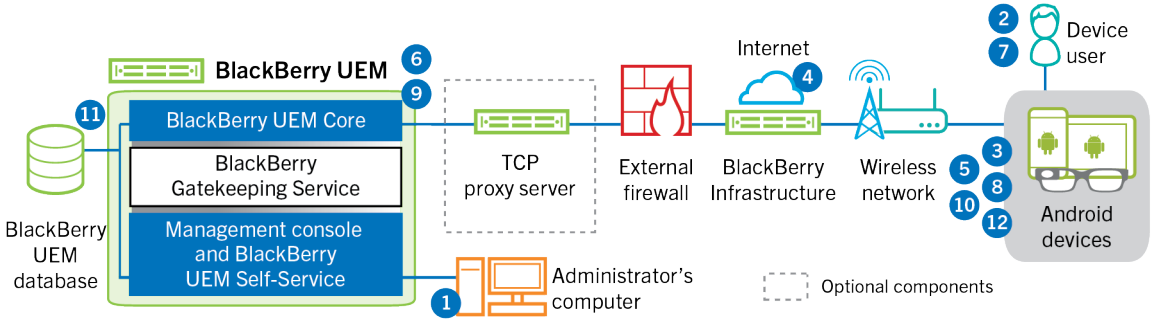
For more information about obtaining and using all of the developer tools available from BlackBerry, visit the BlackBerry Developers site.

Data flows: Activating devices and BlackBerry Dynamics apps

When a user activates a device with BlackBerry UEM, the device is associated with UEM so that you can manage devices and users can access work data on their devices. Device activation types give you different degrees of control over the work and personal data on devices, ranging from full control over all data to specific control over work data only. For more information about activation types and how to activate devices, see the Activating devices Administration content.

This section provides data flows that detail how data travels through your organization's UEM environment when you activate a device or a BlackBerry Dynamics app.

Data flow: Activating an Android Enterprise Work and personal - user privacy device using a managed Google Play account



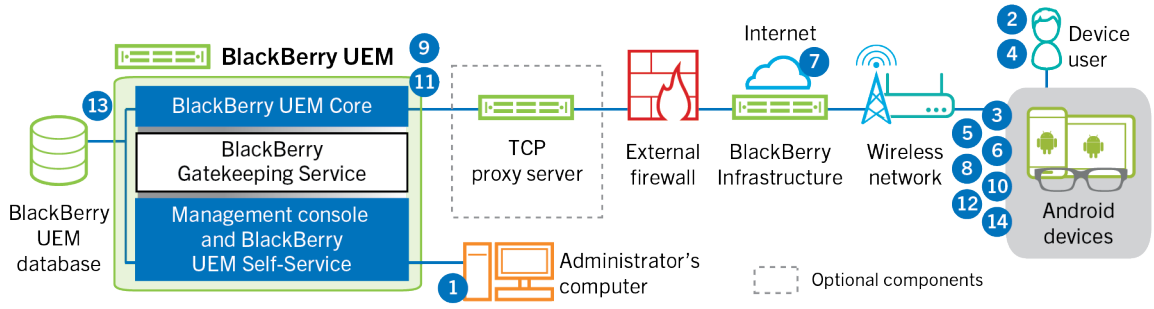
This data flow applies when you allow BlackBerry UEM to manage Google Play accounts.

1. You perform the following actions:
   a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory.
   b. Make sure the "Work and personal - user privacy" activation type is assigned to the user.
   c. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and, optionally, a QR Code and send an email with activation instructions for the user
      - Set a device activation password and communicate the username and password to the user directly or by email
      - Don't set a device activation password and communicate the BlackBerry UEM Self-Service address to the user so that they can set their own activation password and view a QR Code.
2. The user downloads BlackBerry UEM Client from Google Play and installs it on the device. After it is installed, the user opens the BlackBerry UEM Client and enters their email address and activation password or scans the QR Code.
3. The BlackBerry UEM Client on the device performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
4. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user

   b. Retrieves the BlackBerry UEM address for the user
   c. Sends the address to the BlackBerry UEM Client
5. The BlackBerry UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
6. BlackBerry UEM performs the following actions:
   a. Determines the activation type assigned to the user account
   b. Connects to Google and creates a managed Google Play user
   c. Creates a device instance
   d. Associates the device instance with the specified user account
   e. Adds the enrollment session ID to an HTTP session
   f. Sends the user's managed Google Play account information and a successful authentication message to the device
7. If the device is not encrypted, the user is prompted to encrypt the device.
8. The BlackBerry UEM Client performs the following actions:
   a. Connects to Google to verify the user
   b. Creates the work profile on the device
   c. Creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS.
9. BlackBerry UEM performs the following actions:
   a. Validates the client certificate request against the enrollment session ID in the HTTP session
   b. Signs the client certificate request with the root certificate
   c. Sends the signed client certificate and root certificate back to the BlackBerry UEM Client

   A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.
10. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
11. BlackBerry UEM stores the device information in the database and sends the requested configuration information to the device.
12. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating an Android Enterprise Work and personal - full control device using a managed Google Play account



This data flow applies when you allow BlackBerry UEM to manage Google Play accounts.

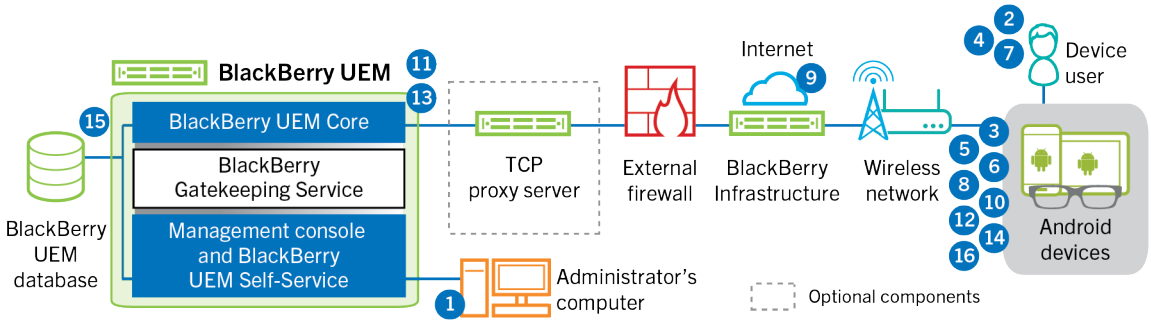
1. You perform the following actions:

   a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory
   b. Make sure that the "Work and personal - full control" activation type is assigned to the user
   c. Allow activation QR codes to include the activation password and the location to download the BlackBerry UEM Client.
2. The user resets their device to the factory default settings.
3. The device restarts and displays a Welcome or Start screen.
4. The user performs the following actions:
   a. Opens the activation email they received on their computer or another device
   b. Taps the device screen seven times to open a QR code reader
   c. Connects the device to a Wi-Fi network
   d. Scans the QR code in the activation email
5. The device performs the following actions:
   a. Prompts the user to encrypt the device and restarts
   b. Downloads the UEM Client from the download location specified by the QR code and installs it
6. The UEM Client performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
7. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BlackBerry UEM server address for the user
   c. Sends the server address to the UEM Client
8. The UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
9. BlackBerry UEM performs the following actions:
   a. Determines the activation type assigned to the user account
   b. Connects to Google and creates a managed Google Play user
   c. Creates a device instance
   d. Associates the device instance with the specified user account
   e. Adds the enrollment session ID to an HTTP session
   f. Sends the user's managed Google Play account information and a successful authentication message to the device
10. The UEM Client performs the following actions:
   a. Connects to Google to verify the user
   b. Creates the work profile on the device
   c. Creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS
11. BlackBerry UEM performs the following actions:
   a. Validates the client certificate request against the enrollment session ID in the HTTP session
   b. Signs the client certificate request with the root certificate
   c. Sends the signed client certificate and root certificate back to the UEM Client

   A mutually authenticated TLS session is established between the UEM Client and BlackBerry UEM.
12. The UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.

13. BlackBerry UEM stores the device information in the database and sends the requested configuration information to the device.
14. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating an Android Enterprise Work space only device using a managed Google Play account



This data flow applies when you allow BlackBerry UEM to manage Google Play accounts.

1. You perform the following actions:
   a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory.
   b. Make sure that the "Work space only" activation type is assigned to the user.
   c. Set the user's activation password.
2. The user resets their device to the factory default settings.
3. The device restarts and prompts the user to select a Wi-Fi network and to add an account.
4. The user enters their Google credentials.
5. The device performs the following actions:
   a. If the device is not encrypted, prompts the user to encrypt the device and restarts
   b. Downloads the BlackBerry UEM Client from Google Play and installs it
6. The BlackBerry UEM Client on the device prompts the user to type their email address and activation password.
7. The user types their email address and activation password or scans the QR Code.
8. The BlackBerry UEM Client performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
9. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BlackBerry UEM server address for the user
   c. Sends the server address to the BlackBerry UEM Client
10. The BlackBerry UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
11. BlackBerry UEM performs the following actions:
   a. Determines the activation type assigned to the user account

b. Connects to Google and creates a managed Google Play user
c. Creates a device instance
d. Associates the device instance with the specified user account
e. Adds the enrollment session ID to an HTTP session
f. Sends the user's managed Google Play account information and a successful authentication message to the device

12. The BlackBerry UEM Client performs the following actions:

a. Connects to Google to verify the user
b. Creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS

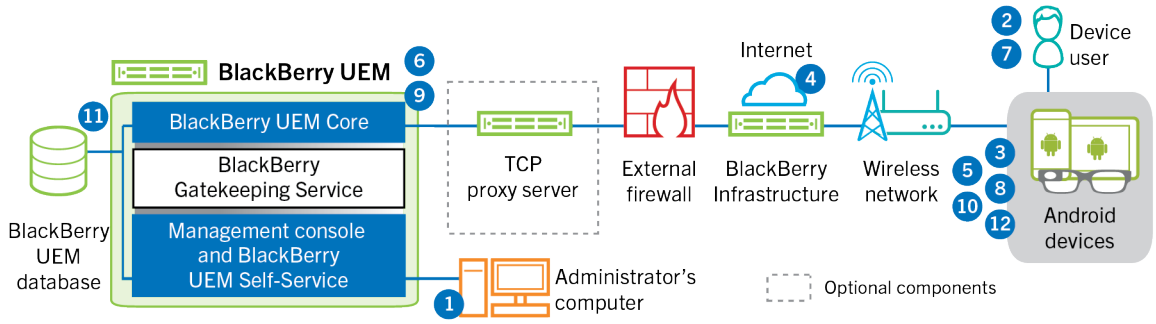
13. BlackBerry UEM performs the following actions:

a. Validates the client certificate request against the enrollment session ID in the HTTP session
b. Signs the client certificate request with the root certificate
c. Sends the signed client certificate and root certificate back to the BlackBerry UEM Client

A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.

14. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
15. BlackBerry UEM stores the device information in the database and sends the requested configuration information to the device.
16. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating an Android Enterprise Work and personal - user privacy device in a Google domain



This data flow applies when BlackBerry UEM is connected to a Google Cloud or Google Workspace domain.

1. You perform the following actions:

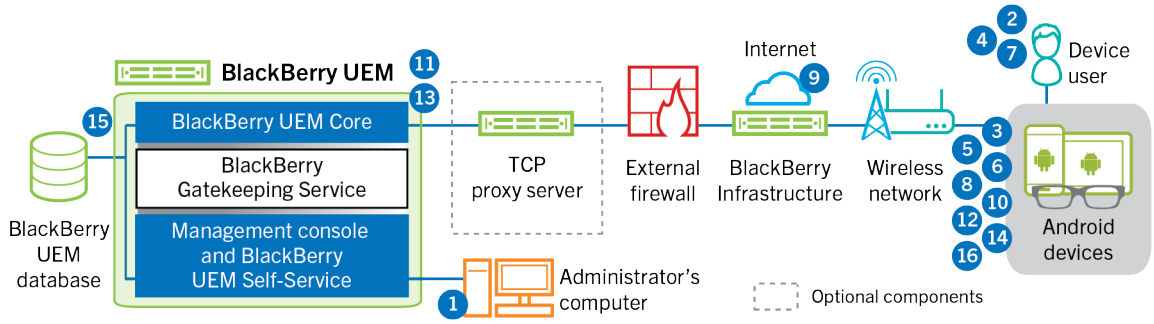
a. Verify that the user has a Google account that is associated with the user's work email address. Optionally, you can configure BlackBerry UEM to create the Google account for the user during the activation process. When BlackBerry UEM creates the account for the user in Google, the user receives an email from the Google domain with their Google account password.
b. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory. When you specify the email address, use the email address that is associated with the user's Google account.
c. Make sure the "Work and personal - user privacy" activation type is assigned to the user.
d. Use one of the following options to provide the user with activation details:

- Automatically generate a device activation password and, optionally, a QR Code and send an email with activation instructions for the user
- Set a device activation password and communicate the username and password to the user directly or by email
- Don't set a device activation password and communicate the BlackBerry UEM Self-Service address to the user so that they can set their own activation password and view a QR Code.

2. The user downloads BlackBerry UEM Client from Google Play and installs it on the device. After it is installed, the user opens the BlackBerry UEM Client and enters their email address and activation password or scans the QR Code.
3. The BlackBerry UEM Client on the device performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
4. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BlackBerry UEM address for the user
   c. Sends the address to the BlackBerry UEM Client
5. The BlackBerry UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
6. BlackBerry UEM performs the following actions:
   a. Determines the activation type assigned to the user account
   b. Connects to the managed Google domain to verify the user information. If the user does not exist, depending on your configuration, BlackBerry UEM may create the user in the Google domain.
   c. Creates a device instance
   d. Associates the device instance with the specified user account
   e. Adds the enrollment session ID to an HTTP session
   f. Sends a successful authentication message to the device
7. If the device is not encrypted, the user is prompted to encrypt the device.
8. The BlackBerry UEM Client performs the following actions:
   a. Creates the work profile on the device
   b. Prompts the user for the user's Google account information
   c. Connects to the managed Google domain to authenticate the user
   d. Creates the work profile on the device
   e. Creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS.
9. BlackBerry UEM performs the following actions:
   a. Validates the client certificate request against the enrollment session ID in the HTTP session
   b. Signs the client certificate request with the root certificate
   c. Sends the signed client certificate and root certificate back to the BlackBerry UEM Client

   A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.
10. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
11. BlackBerry UEM stores the device information and sends the requested configuration information to the device.
12. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating an Android Enterprise Work and personal - full control device in a Google domain



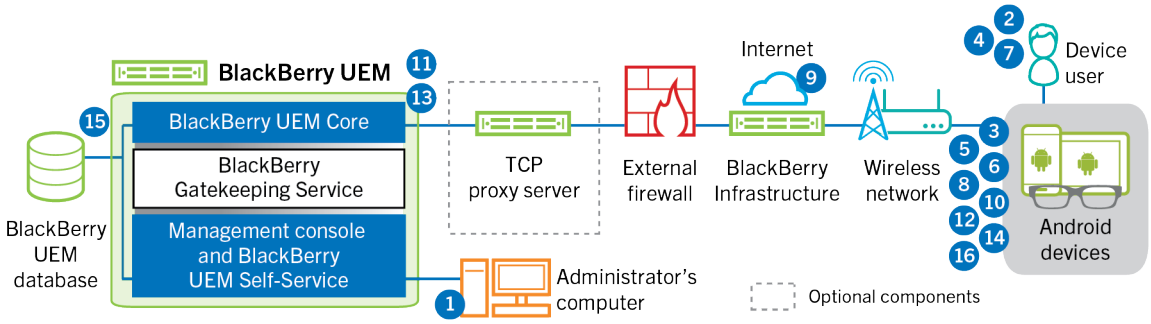
This data flow applies when BlackBerry UEM is connected to a Google Cloud or Google Workspace domain.

1. You perform the following actions:
   a. Verify that the user has a Google account that is associated with the user's work email address. Optionally, you can configure BlackBerry UEM to create the Google account for the user during the activation process. When BlackBerry UEM creates the account for the user in Google, the user receives an email from the Google domain with their Google account password.
   b. Verify that the "Enforce EMM Policy" setting is enabled for the Google domain. This setting specifies that activated devices are managed by an EMM provider, such as BlackBerry UEM.
   c. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory. When you specify the email address, use the email address that is associated with the user's Google account.
   d. Make sure that the "Work and personal - full control" activation type is assigned to the user.
   e. Set the user's activation password.
2. The user resets their device to the factory default settings.
3. The device restarts and prompts the user to select a Wi-Fi network and to add an account.
4. The user enters their work email address and password.
5. The device communicates with the Google domain to verify that the user is a work user and to check if the Enforce EMM Policy setting is enabled. After the device performs the appropriate validations, the device performs the following actions:
   a. If the device is not encrypted, prompts the user to encrypt the device and restarts
   b. Downloads the BlackBerry UEM Client from Google Play and installs it
6. The BlackBerry UEM Client on the device prompts the user to type their email address and activation password.
7. The user types their email address and activation password or scans the QR Code.
8. The BlackBerry UEM Client on the device performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
9. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BlackBerry UEM server address for the user
   c. Sends the server address to the BlackBerry UEM Client

10. The BlackBerry UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
11. BlackBerry UEM performs the following actions:
    a. Determines the activation type assigned to the user account
    b. Connects to the Google domain to verify the user information. If the user does not exist, depending on your configuration, BlackBerry UEM may create the user in the Google domain
    c. Creates a device instance
    d. Associates the device instance with the specified user account
    e. Adds the enrollment session ID to an HTTP session
    f. Sends a successful authentication message to the device
12. The BlackBerry UEM Client performs the following actions:
    a. Creates the work profile on the device
    b. Prompts the user for the user's Google account information
    c. Connects to the Google domain to authenticate the user
    d. Creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS
13. BlackBerry UEM performs the following actions:
    a. Validates the client certificate request against the enrollment session ID in the HTTP session
    b. Signs the client certificate request with the root certificate
    c. Sends the signed client certificate and root certificate back to the BlackBerry UEM Client

    A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.
14. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
15. BlackBerry UEM stores the device information and sends the requested configuration information to the device.
16. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating an Android Enterprise Work space only device in a Google domain



This data flow applies when BlackBerry UEM is connected to a Google Cloud or Google Workspace domain.

1. You perform the following actions:

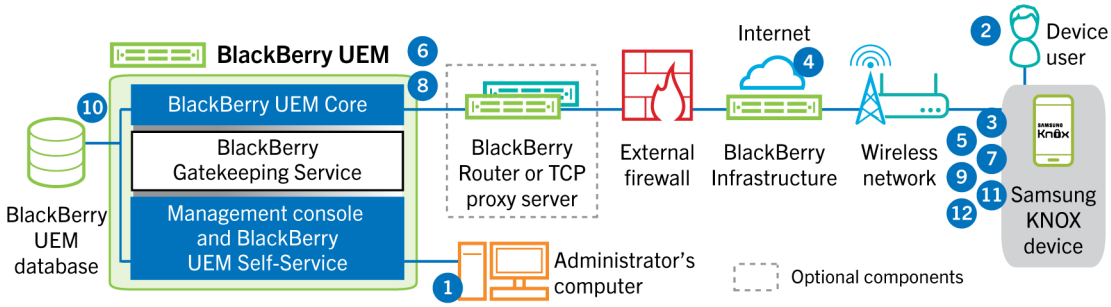
   a. Verify that the user has a Google account that is associated with the user's work email address. Optionally, you can configure BlackBerry UEM to create the Google account for the user during the activation process. When BlackBerry UEM creates the account for the user in Google, the user receives an email from the Google domain with their Google account password.
   b. Verify that the "Enforce EMM Policy" setting is enabled for the Google domain. This setting specifies that activated devices are managed by an EMM provider, such as BlackBerry UEM.
   c. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory. When you specify the email address, use the email address that is associated with the user's Google account.
   d. Make sure that the "Work space only" activation type is assigned to the user.
   e. Set the user's activation password.
2. The user resets their device to the factory default settings.
3. The device restarts and prompts the user to select a Wi-Fi network and to add an account.
4. The user enters their work email address and password.
5. The device communicates with the Google domain to verify that the user is a work user and to check if the Enforce EMM Policy setting is enabled. After the device performs the appropriate validations, the device performs the following actions:
   a. If the device is not encrypted, prompts the user to encrypt the device and restarts
   b. Downloads the BlackBerry UEM Client from Google Play and installs it
6. The BlackBerry UEM Client on the device prompts the user to type their email address and activation password.
7. The user types their email address and activation password or scans the QR Code.
8. The BlackBerry UEM Client on the device performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
9. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BlackBerry UEM server address for the user
   c. Sends the server address to the BlackBerry UEM Client
10. The BlackBerry UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
11. BlackBerry UEM performs the following actions:
   a. Determines the activation type assigned to the user account
   b. Connects to the Google domain to verify the user information. If the user does not exist, depending on your configuration, BlackBerry UEM may create the user in the Google domain.
   c. Creates a device instance
   d. Associates the device instance with the specified user account
   e. Adds the enrollment session ID to an HTTP session
   f. Sends a successful authentication message to the device
12. The BlackBerry UEM Client performs the following actions:
   a. Prompts the user for the user's Google account information
   b. Connects to the Google domain to authenticate the user
   c. Creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS
13. BlackBerry UEM performs the following actions:
   a. Validates the client certificate request against the enrollment session ID in the HTTP session

b. Signs the client certificate request with the root certificate
c. Sends the signed client certificate and root certificate back to the BlackBerry UEM Client

A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.

14. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
15. BlackBerry UEM stores the device information and sends the requested configuration information to the device.
16. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating a device to use Knox Workspace



1. You perform the following actions:
   a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory
   b. Make sure the "Work and personal - full control (Samsung Knox)", "Work and personal - user privacy (Samsung Knox)", or "Work space only - (Samsung Knox)" activation type is assigned to the user
   c. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and, optionally, a QR Code and send an email with activation instructions for the user
      - Set a device activation password and communicate the username and password to the user directly or by email
      - Don't set a device activation password and communicate the BlackBerry UEM Self-Service address to the user so that they can set their own activation password and view a QR Code.
2. The user downloads and installs the BlackBerry UEM Client on the device. After it is installed, the user opens the BlackBerry UEM Client and enters the email address and activation password or scans the QR Code.
3. The BlackBerry UEM Client performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
4. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BlackBerry UEM address for the user
   c. Sends the address to the BlackBerry UEM Client
5. The BlackBerry UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
6. BlackBerry UEM performs following actions:

a. Inspects the credentials for validity
b. Creates a device instance
c. Associates the device instance with the specified user account in the BlackBerry UEM database
d. Adds the enrollment session ID to an HTTP session
e. Sends a successful authentication message to the device

7. The BlackBerry UEM Client creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS.
8. BlackBerry UEM performs the following actions:

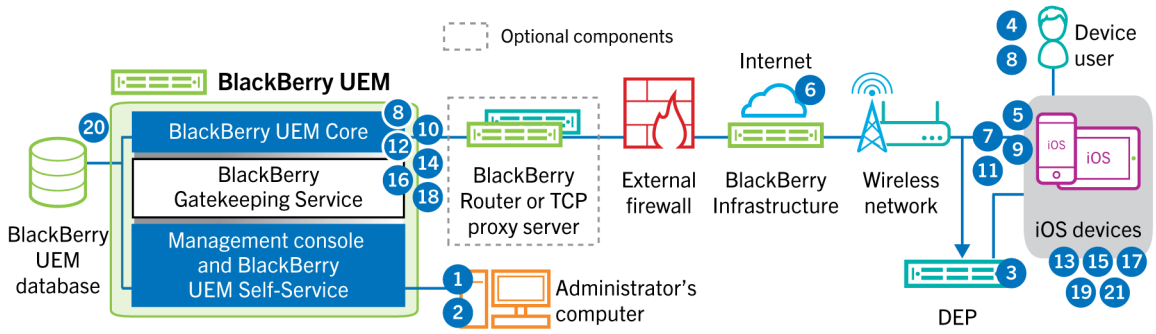
   a. Validates the client certificate request against the enrollment session ID in the HTTP session
   b. Signs the client certificate request with the root certificate
   c. Sends the signed client certificate and root certificate back to the BlackBerry UEM Client

   A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.
9. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
10. BlackBerry UEM stores the device information in the database and sends the requested configuration information to the device.
11. The BlackBerry UEM Client determines if the device uses Knox Workspace and is running a supported version. If the device uses Knox Workspace, the device connects to the Samsung infrastructure and activates the Knox management license. After it is activated, the BlackBerry UEM Client applies the Knox MDM and Knox Workspace IT policy rules.
12. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

After the activation is complete, the user is prompted to create a work space password for the Knox Workspace. Data in the Knox Workspace is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint.

Note: If the device is activated with the "Work space only - (Samsung Knox)" activation type, the personal space is removed when the Knox Workspace is set up.

Data flow: Activating an iOS device



1. If you plan to use the Apple Device Enrollment Program, you perform the following actions:

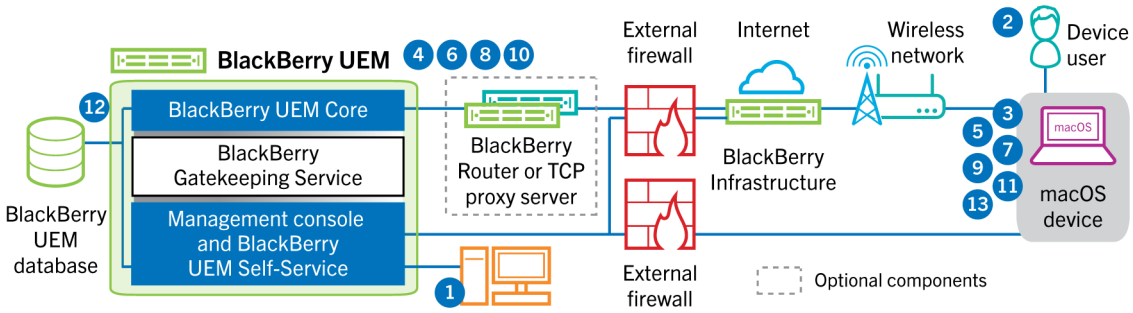
   a. Make sure that BlackBerry UEM is configured to synchronize with DEP
   b. Register the device in DEP and assign it to an MDM server
   c. Assign an enrollment configuration to the device
2. You perform the following actions:

   a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory
   b. Assign an activation profile to the user
   c. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and, optionally, a QR Code and send an email with activation instructions for the user
      - Set a device activation password and communicate the username and password to the user directly or by email
      - Don't set a device activation password and communicate the BlackBerry UEM Self-Service address to the user so that they can set their own activation password and view a QR Code.
3. If the device is registered in the Apple DEP, the device communicates with the Apple DEP web service during its initial setup. If you configured the device to install the BlackBerry UEM Client app, the device automatically downloads and installs it.
4. If the device is not registered in the Apple DEP or if you did not configure the device to install the BlackBerry UEM Client, the user manually downloads and installs the BlackBerry UEM Client on the device. After it is installed, the user opens the BlackBerry UEM Client and enters the email address and activation password or scans the QR Code.
5. The BlackBerry UEM Client performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends a request for activation information to the BlackBerry Infrastructure
6. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BlackBerry UEM address for the user
   c. Sends the address to the BlackBerry UEM Client
7. The BlackBerry UEM Client establishes a connection with BlackBerry UEM using an HTTP CONNECT call over port 443 and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
8. BlackBerry UEM performs following actions:
   a. Inspects the credentials for validity
   b. Creates a device instance
   c. Associates the device instance with the specified user account in the BlackBerry UEM database
   d. Adds the enrollment session ID to an HTTP session
   e. Sends a successful authentication message to the device
9. The BlackBerry UEM Client creates a CSR using the information received from BlackBerry UEM and sends a client certificate request over HTTPS.
10. BlackBerry UEM performs the following actions:
    a. Validates the client certificate request against the enrollment session ID in the HTTP session
    b. Signs the client certificate request with the root certificate
    c. Sends the signed client certificate and root certificate back to the BlackBerry UEM Client

    A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.
11. The BlackBerry UEM Client displays a message to inform the user that a certificate must be installed to complete the activation. The user clicks OK and is redirected to the link for the native MDM Daemon activation. The BlackBerry UEM Client establishes a connection to BlackBerry UEM.
12. BlackBerry UEM provides the MDM profile to the device. This profile contains the MDM activation URL and the challenge. The MDM profile is wrapped as a PKCS#7 signed message that includes the full certificate chain of the signer, which allows the device to validate the profile. This triggers the enrollment process.

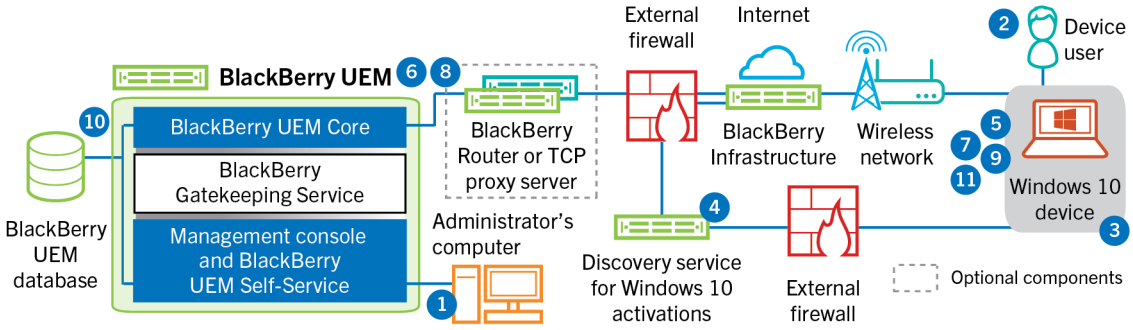
13. The native MDM Daemon on the device sends the device profile, including the customer ID, language, and OS version, to BlackBerry UEM.
14. BlackBerry UEM validates that the request is signed by a CA and responds to the native MDM Daemon with a successful authentication notification.
15. The native MDM Daemon sends a request to BlackBerry UEM asking for the CA certificate, CA capabilities information, and a device-issued certificate.
16. BlackBerry UEM sends the CA certificate, CA capabilities information, and the device-issued certificate to the native MDM Daemon.
17. The native MDM Daemon installs the MDM profile on the device. The BlackBerry UEM Client notifies BlackBerry UEM of the successful installation of the MDM profile and certificate and polls BlackBerry UEM periodically until it acknowledges that the MDM activation is complete.
18. BlackBerry UEM acknowledges that the MDM activation is complete.
19. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
20. BlackBerry UEM stores the device information in the database and sends configuration information to the device.
21. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration updates. The activation process is complete.

Data flow: Activating a macOS device



1. You make sure that the user has a BlackBerry UEM user account and the login information for BlackBerry UEM Self-Service, including:
   - Web address for BlackBerry UEM Self-Service
   - Username and password
   - Domain name
2. The user logs in to BlackBerry UEM Self-Service on their macOS device and activates the device.
3. The device sends an activation request to BlackBerry UEM on port 443.
4. BlackBerry UEM provides the MDM profile to the device. This profile contains the MDM activation URL and the challenge. The MDM profile is wrapped as a PKCS#7 signed message that includes the full certificate chain of the signer, which allows the device to validate the profile. This triggers the enrollment process.
5. The native MDM Daemon on the device sends the device profile, including the customer ID, language, and OS version, to BlackBerry UEM.
6. BlackBerry UEM validates that the request is signed by a CA and responds to the native MDM Daemon with a successful authentication notification.
7. The native MDM Daemon sends a request to BlackBerry UEM asking for the CA certificate, CA capabilities information, and a device issued certificate.
8. BlackBerry UEM sends the CA certificate, CA capabilities information, and the device issued certificate to the native MDM Daemon.
9. The native MDM Daemon installs the MDM profile on the device.
10. BlackBerry UEM acknowledges that the MDM activation is complete.
11. The device requests all configuration information.
12. BlackBerry UEM stores the device information in the database and sends configuration information to the device.
13. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating a Windows 10 device



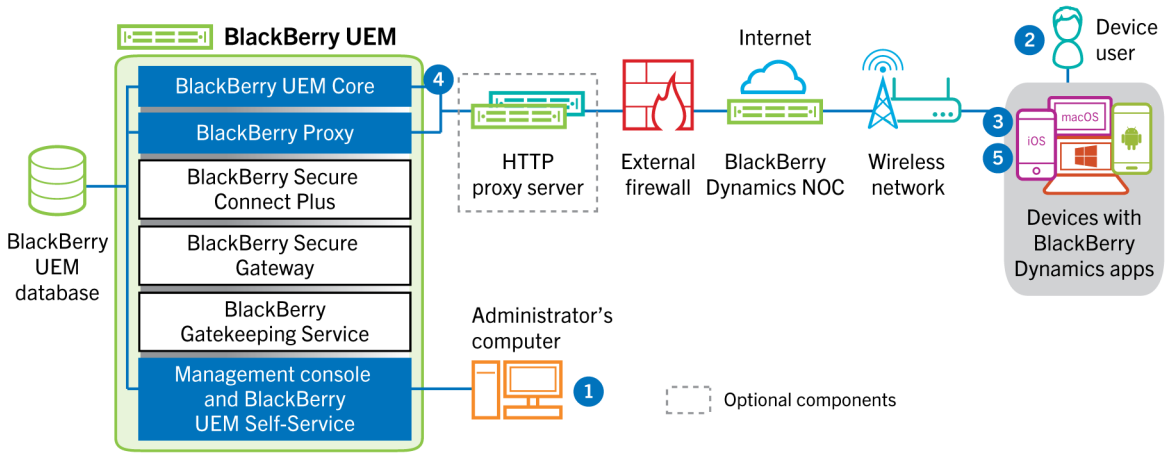
1. You perform the following actions:
   a. Configure the discovery service to simplify Windows 10 activations
   b. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory
   c. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and send an email with activation instructions for the user.
      - Set a device activation password and select the option to send the activation information to the user by email.
      - Don't set a device activation password and communicate the BlackBerry UEM Self-Service address to the user so that they can set their own activation password and view their server address.
   d. Provide the user a CA certificate generated by BlackBerry UEM to install on their device
2. The user completes the following actions on their device:
   a. Checks that the device has Internet connectivity on port 443
   b. Opens and installs the certificate
   c. Navigates to Settings > Accounts > Work access and taps Connect
   d. When prompted, enters their email address and activation password they received on the activation email
3. The device establishes a connection to the discovery service that you configured to simplify Windows 10 activations in your organization.
4. The discovery service checks that the SRP ID for the BlackBerry UEM server is valid and redirects the device to BlackBerry UEM.
5. The device sends an activation request to BlackBerry UEM on port 443. The activation request includes the username, password, device operating system, and unique device identifier.
6. BlackBerry UEM performs following actions:
   a. Inspects the credentials for validity
   b. Creates a device instance
   c. Associates the device instance with the specified user account in the BlackBerry UEM database
   d. Adds the enrollment session ID to an HTTP session
   e. Sends a successful authentication message to the device
7. The device creates a CSR and sends it to BlackBerry UEM over HTTPS. The CSR contains the username and activation password.
8. BlackBerry UEM validates the username and password, validates the CSR, and returns the client certificate and the CA certificate to the device.

All communication between the device and BlackBerry UEM is now mutually authenticated end to end using these certificates.

9. The device requests all configuration information.
10. BlackBerry UEM stores the device information in the database and sends configuration information to the device.
11. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating a BlackBerry Dynamics app for the first time on a device

This data flow describes how data travels when a BlackBerry Dynamics app is activated on a device and no other BlackBerry Dynamics app nor the BlackBerry UEM Client is already activated.

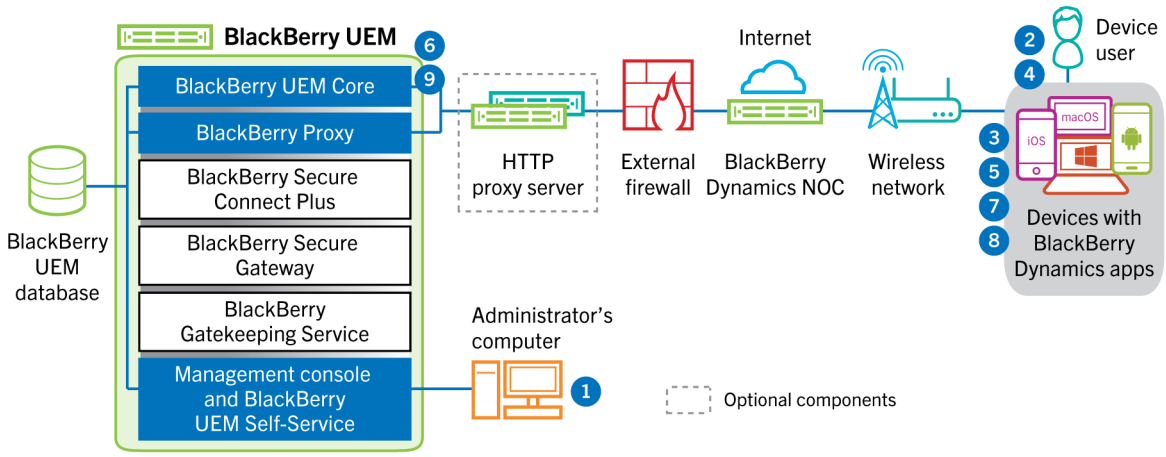


1. An administrator performs the following actions:
   a. Assigns one or more BlackBerry Dynamics apps to a user.
   b. Issues activation credentials (access key, activation password, or QR code) or using a third-party identity provider, and sends them to the user or instructs the user to generate credentials from BlackBerry UEM Self-Service.
2. The user performs the following actions:
   a. Installs the app on the device.
   b. Obtains and enters the provided activation credentials .
3. The BlackBerry Dynamics app performs the following actions:
   a. Connects to the BlackBerry Dynamics NOC and completes activation.
   b. Obtains the BlackBerry UEM address using one of the following methods:
      - If the user manually entered the credentials, the app fetches the address from the BlackBerry Infrastructure.
      - If the user scanned a QR Code, the app receives the address from the QR code.
   c. Connects to BlackBerry UEM through the BlackBerry Infrastructure and establishes an end-to-end encrypted session with BlackBerry UEM using the EC-SPEKE protocol.

      This session can only be decrypted by the BlackBerry UEM instance that issued the activation credentials.
   d. Sends the activation request over the secured session.
4. BlackBerry UEM verifies the activation request and sends encrypted activation response to the app. The activation response includes data required by the app to communicate with BlackBerry UEM, including a client certificate, master session key, list of BlackBerry Proxy instances, and trusted certificate authorities.
5. The app prompts the user to set a password for the app and register it as an easy activation delegate with the BlackBerry Dynamics NOC to allow subsequent BlackBerry Dynamics app to be activated on the device without the user manually obtaining new credentials.

Data flow: Activating a BlackBerry Dynamics app when one is already activated on the device

This data flow describes how data travels when a BlackBerry Dynamics app is activated on a device and the BlackBerry UEM Client or another BlackBerry Dynamics app is already activated and acts as an easy activation delegate.



1. An administrator assigns one or more BlackBerry Dynamics apps to a user.
2. The user installs the app on the device.
3. The app performs the following actions:
   a. Queries the BlackBerry Dynamics NOC and identifies another app that is activated on the device
   b. Requests the activation credentials from the previously activated app
4. The user approves the activation request from the previously activated app on the device.
5. The previously activated app sends the credentials to BlackBerry UEM.
6. BlackBerry UEM sends the credentials request and BlackBerry UEM URL to the existing app.
7. The previously activated app returns the credentials and the URL to the new app.
8. The new app completes the following actions:
   a. Activates with the BlackBerry Dynamics NOC
   b. Connects to BlackBerry UEM through the BlackBerry Infrastructure and establishes an end-to-end encrypted session with BlackBerry UEM using the EC-SPEKE protocol.

      This session can only be decrypted by the BlackBerry UEM instance that issued the activation credentials.
   c. Sends the activation request through the secured session
9. BlackBerry UEM verifies the activation request and sends encrypted activation response to the app. The activation response includes data required by the app to communicate with BlackBerry UEM, including a client certificate, master session key, list of BlackBerry Proxy instances, and trusted certificate authorities.

Data flows: Sending and receiving work data

When devices that are active on BlackBerry UEM send and receive work data, they connect to your organization's mail, application, or content servers. For example, when they use the work email or calendar apps, devices establish a connection to your organization's mail server. When they use the work browser to navigate the intranet, devices establish a connection to the web server in your organization, and so on.

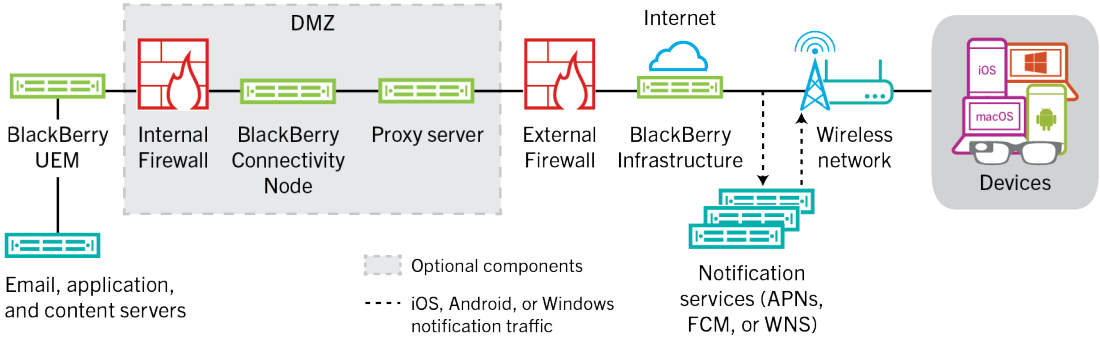
This section provides data flows that detail how work data travels through your organization's UEM environment.

Depending on the type of device, the activation type, license types, and configuration settings, a device may establish connections to your organization's servers using the following paths:

Data Path	Description
Work Wi-Fi network	You can use UEM to configure Wi-Fi profiles for devices so that devices can connect to your organization's resources using your work Wi-Fi network.
VPN	You can use UEM to configure VPN profiles for devices or users may configure VPN profiles on their devices so that devices can connect to your organization's resources using a VPN.
UEM and the BlackBerry Infrastructure or BlackBerry Dynamics NOC	Depending on the device, activation, and license type, and on the presence of BlackBerry Dynamics apps, devices may be able to use enterprise connectivity to communicate with your organization's resources through UEM and the BlackBerry Infrastructure. • For iOS devices, if the devices have an appropriate license, you can enable the BlackBerry Secure Gateway to allow devices to connect to your work mail server through the BlackBerry Infrastructure and 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 iOS devices to connect to Microsoft Exchange when they are not connected to your VPN or work Wi-Fi network. • For iOS, Android Enterprise, and Samsung Knox Workspace devices, if the devices have an appropriate license, you can use enterprise connectivity by enabling BlackBerry Secure Connect Plus. When devices use BlackBerry Secure Connect Plus, work data travels in a secure IP tunnel established between apps on the device and your organization's network through the BlackBerry Infrastructure. • BlackBerry Dynamics apps installed on devices communicate with BlackBerry Proxy. Depending on your configuration, data can travel through the BlackBerry Dynamics NOC or BlackBerry Infrastructure or can bypass them using BlackBerry Dynamics Direct Connect. • Devices can use enterprise connectivity for all work data. Enterprise connectivity encrypts and authenticates all work data and sends it through UEM and the BlackBerry Infrastructure. Enterprise connectivity limits the number of ports that you need to open on your organization's external firewall to a single port, 3101.

Sending and receiving work data using the BlackBerry Infrastructure

Devices connect to BlackBerry UEM through the BlackBerry Infrastructure to obtain configuration updates and to send and receive work data using enterprise connectivity or the BlackBerry Secure Gateway. The following diagram shows how devices connect to BlackBerry UEM and your organization's resources through the BlackBerry Infrastructure.



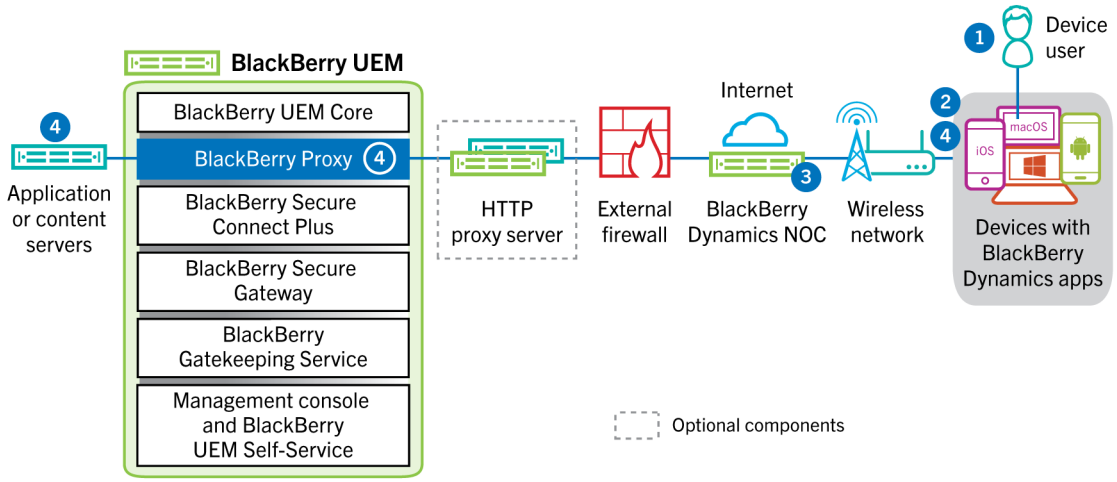
The following table lists the circumstances when devices connect to BlackBerry UEM and your organization's network through the BlackBerry Infrastructure.

Device type	Description
All devices	All devices use this communication path to send and receive configuration data, such as device commands, policy and profile updates, and to send device information and activity reports. For more information, see Data flows: Receiving device configuration updates.
iOS devices	You can enable the BlackBerry Secure Gateway to allow iOS devices to connect to your work mail 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 to receive work email when they are not connected to your organization's VPN or work Wi-Fi network.
iOS, Android Enterprise, and Samsung Knox Workspace, devices.	Devices that have an enterprise connectivity profile configured to use BlackBerry Secure Connect Plus can use a secure IP tunnel through the BlackBerry Infrastructure to transfer data between apps and your organization's network. For iOS devices, BlackBerry Secure Connect Plus can provide a secure tunnel between your organization's network and all apps or only specified apps. For Android Enterprise devices, BlackBerry Secure Connect Plus provides a secure tunnel between all work space apps and your organization's network. For Samsung Knox Workspace devices, BlackBerry Secure Connect Plus can provide a secure tunnel between your organization's network and all work apps or only specified work apps.

Device type	Description
iOS and Android devices with BlackBerry Dynamics apps installed	Enterprise connectivity for BlackBerry Dynamics apps does not use the BlackBerry Infrastructure. Instead, data in transit between BlackBerry Dynamics apps and BlackBerry Proxy can travel through the BlackBerry Dynamics NOC or can bypass the NOC using BlackBerry Dynamics Direct Connect.

Data flow: Sending and receiving work data from a BlackBerry Dynamics app through the BlackBerry Dynamics NOC

This data flow describes how data travels when a BlackBerry Dynamics app accesses an application or content server in your organization through the BlackBerry Dynamics NOC and BlackBerry UEM.

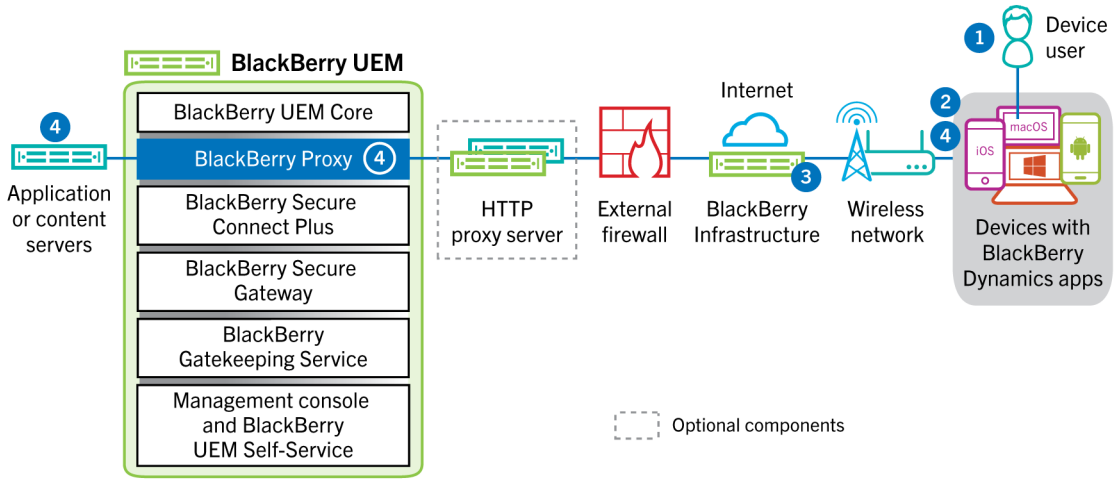


1. The user opens a BlackBerry Dynamics app to access work data.
2. The BlackBerry Dynamics app establishes a connection to the BlackBerry Dynamics NOC. The connection is authenticated with the master link key that was created when the app was activated.
3. The BlackBerry Dynamics NOC communicates with BlackBerry Proxy over a pre-established secure connection to establish an end-to-end connection between the BlackBerry Dynamics app and BlackBerry Proxy that carries the work data. The work data is encrypted with a session key that is not known to the BlackBerry Dynamics NOC.
4. When the secure end-to-end connection is established, work data can travel between the device and application or content servers behind the firewall via BlackBerry Proxy.

Data flow: Sending and receiving work data from a BlackBerry Dynamics app through the BlackBerry Infrastructure

Depending on your server configuration, work data for apps developed with BlackBerry Dynamics SDK 7.0 and later may travel through the BlackBerry Infrastructure rather than the BlackBerry Dynamics NOC. If you have a new installation of BlackBerry UEM version 12.12, BlackBerry UEM uses the BlackBerry Infrastructure by default. If you upgraded from a previous version of BlackBerry UEM, you must contact BlackBerry Technical Support if you want to enable this feature.

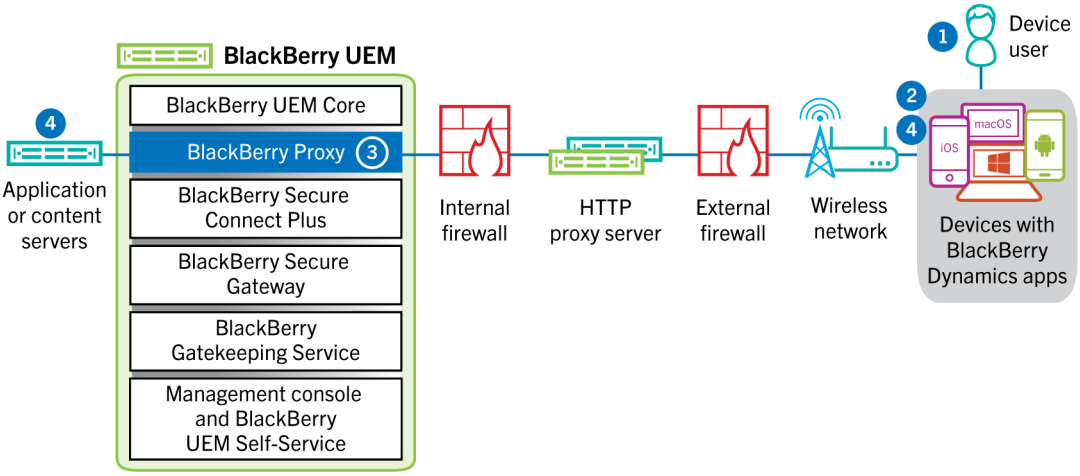
This data flow describes how data travels when a BlackBerry Dynamics app accesses an application or content server in your organization through the BlackBerry Infrastructure and BlackBerry UEM.



1. The user opens a BlackBerry Dynamics app to access work data.
2. The BlackBerry Dynamics app establishes a connection to the BlackBerry Infrastructure.
3. The BlackBerry Infrastructure communicates with BlackBerry Proxy over a pre-established TLS connection.
4. The BlackBerry Dynamics app establishes a TLS connection to the BlackBerry Proxy and work data is exchanged over a secure end-to-end connection.

Data flow: Sending and receiving work data from a BlackBerry Dynamics app using BlackBerry Dynamics Direct Connect

This data flow describes how data travels when a BlackBerry Dynamics app accesses an application or content server in your organization through BlackBerry Dynamics Direct Connect and BlackBerry UEM. For more information on Direct Connect, see Configuring Direct Connect with BlackBerry UEM.

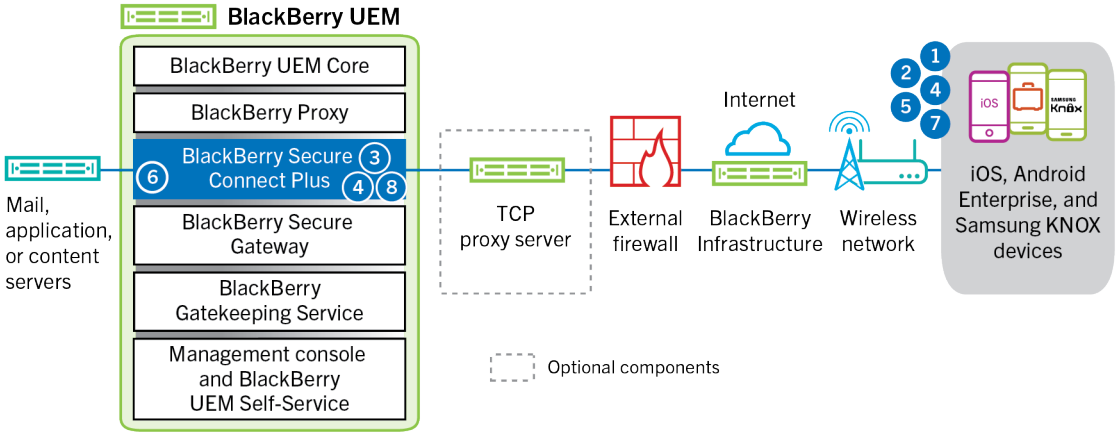


1. The user opens a BlackBerry Dynamics app to access work data.
2. The BlackBerry Dynamics app establishes a TLS connection to BlackBerry Proxy.
3. BlackBerry Proxy authenticates with the BlackBerry Dynamics app. BlackBerry Proxy authenticates with the app using its server certificate. BlackBerry Proxy validates the app using a MAC keyed with a session key known only to BlackBerry Proxy and the app.
4. When the secure end-to-end connection is established, work data can travel between the device and application or content servers behind the firewall via BlackBerry Proxy.

Data flow: Accessing an application or content server using BlackBerry Secure Connect Plus

This data flow describes how data travels when an app on a device that is configured to use BlackBerry Secure Connect Plus accesses an application or content server in your organization.

This data flow does not apply to BlackBerry Dynamics apps in the work space on Android Enterprise devices or Samsung Knox Workspace devices. For more information see, Data flow: Sending and receiving work data from a BlackBerry Dynamics app on an Android device using BlackBerry Secure Connect Plus



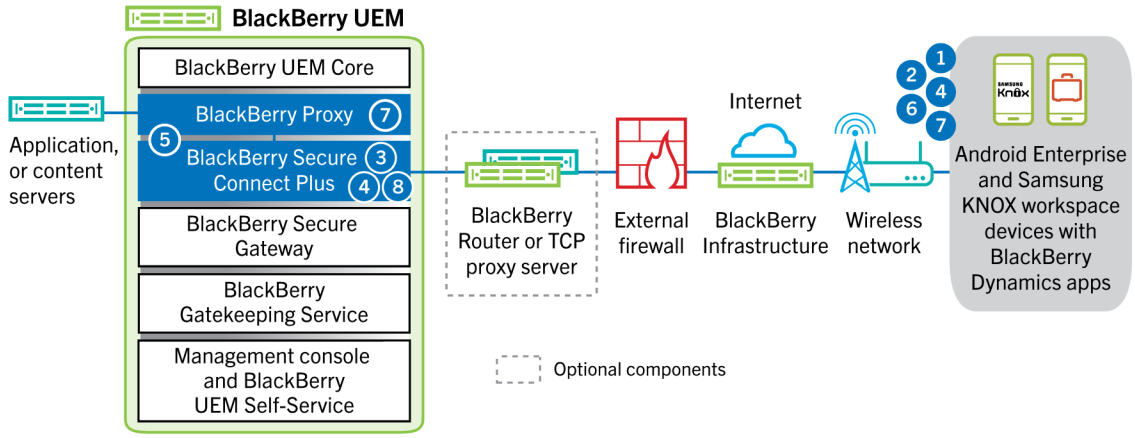
1. The user opens an app to access work data from a content or application server behind your organization's firewall.
   - For Android Enterprise devices, all work space apps except those you choose to restrict use BlackBerry Secure Connect Plus.
   - For Samsung Knox Workspace devices, you specify whether all work space apps or only specified work apps use BlackBerry Secure Connect Plus.
   - For iOS devices, you specify whether all apps or only specified apps use BlackBerry Secure Connect Plus.
2. The device sends a requests through a TLS tunnel, over port 443, to the BlackBerry Infrastructure to request a secure tunnel to the work network. The signal is encrypted by default using FIPS-140 certified Certicom libraries. The signaling tunnel is encrypted end-to-end.
3. BlackBerry Secure Connect Plus receives the request from the BlackBerry Infrastructure through port 3101.
4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.
5. The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).
6. BlackBerry Secure Connect Plus transfers the IP data to and from your organization's network. BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified Certicom libraries.
7. The app receives and displays the data on the device.
8. As long as the tunnel is open, supported apps use it to access network resources. When the tunnel is no longer the best available method to connect to your organization's network, BlackBerry Secure Connect Plus terminates it.

Data flow: Sending and receiving work data from a BlackBerry Dynamics app on an Android device using BlackBerry Secure Connect Plus

This data flow describes how data travels when a BlackBerry Dynamics app on an Android Enterprise or Samsung Knox Workspace device uses BlackBerry Secure Connect Plus.

If you are using BlackBerry Secure Connect Plus with BlackBerry Dynamics apps on an Android Enterprise device, it is recommended that you restrict BlackBerry Dynamics apps from using BlackBerry Secure Connect Plus to avoid network latency. You can't restrict specific apps on Samsung Knox Workspace devices.

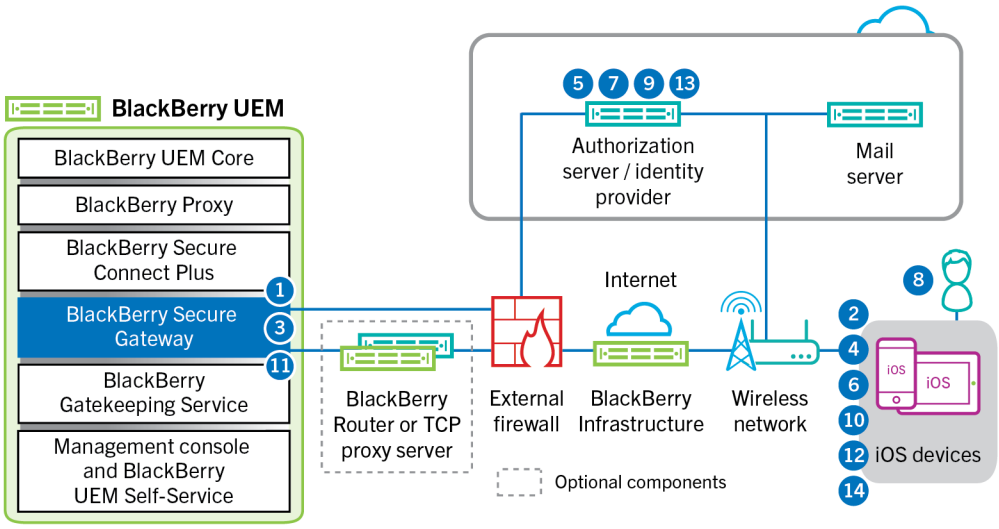
If you are using BlackBerry Secure Connect Plus with BlackBerry Dynamics apps on an Android Enterprise device or a Samsung Knox Workspace device, it is recommended that you configure BlackBerry UEM not to send BlackBerry Dynamics app data through the BlackBerry Dynamics NOC to reduce network latency.



1. The user opens a BlackBerry Dynamics app to access work data.
2. The device sends a request through a TLS tunnel, over port 443, to the BlackBerry Infrastructure to request a secure tunnel to the work network. The signal is encrypted by default using FIPS-140 certified Certicom libraries. The signaling tunnel is encrypted end to end.
3. BlackBerry Secure Connect Plus receives the request from the BlackBerry Infrastructure through port 3101.
4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel for the device through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end to end with DTLS.
5. BlackBerry Secure Connect Plus establishes a connection with BlackBerry Proxy.
6. The BlackBerry Dynamics app establishes a connection to BlackBerry Proxy using the BlackBerry Secure Connect Plus tunnel.
7. BlackBerry Proxy authenticates with the BlackBerry Dynamics app using its server certificate. BlackBerry Proxy validates the app using a MAC keyed with a session key known only to BlackBerry Proxy and the app.
8. When the secure connection is established between BlackBerry Proxy and the app, work data can travel between the device and application or content servers behind the firewall using the BlackBerry Secure Connect Plus tunnel to BlackBerry Proxy. BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified Certicom libraries.

Data flow: Authenticating with the mail server from an iOS device when using BlackBerry Secure Gateway

This data flow describes how iOS devices authenticate with your mail server through BlackBerry Secure Gateway using Microsoft modern authentication.



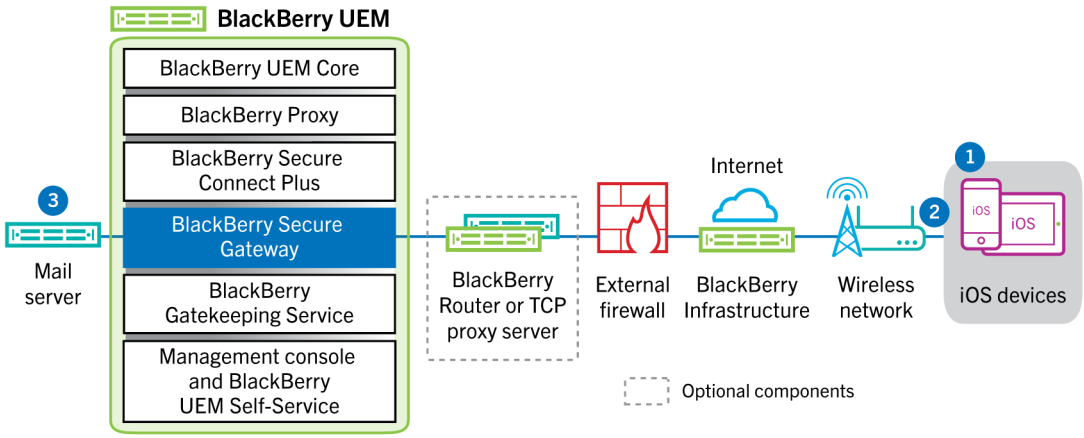
The following steps describe the standard data flow. Some details may vary depending on the configuration of your Entra tenant. For more information on how the Microsoft identity provider manages authorization requests, see the Microsoft documentation.

1. BlackBerry Secure Gateway retrieves and caches the discovery documents from the authorization server/identity provider specified in the BlackBerry Secure Gateway configuration settings. BlackBerry Secure Gateway retrieves both the unversioned discovery document for iOS 13 devices and the v2.0 discovery document for iOS 14.6 and later devices.
2. The device establishes a secure connection through the BlackBerry Infrastructure to the BlackBerry Secure Gateway.
3. The BlackBerry Secure Gateway establishes a TLS connection with the authorization server/identity provider specified in the BlackBerry Secure Gateway configuration settings.
4. The device sends an authorization code request through the BlackBerry Secure Gateway to the authorization server/identity provider.
5. The authorization server/identity provider returns a 302 HTTP redirect response to the device.
6. The device sends an authorization request to the URL specified by the redirect response. The request does not route through the BlackBerry Secure Gateway.
7. The authorization server/identity provider sends user authentication request to the device. The type of request (for example, a login page, or prompt from the Microsoft Authenticator app) and the message flow for user authentication depends on the configuration of your Entra tenant.
8. The user provides the requested credentials to the authorization server/identity provider.
9. When user authentication is complete, the authorization server/identity provider sends an authorization code to the device.
10. The device requests the authorization server/identity provider discovery document from the BlackBerry Secure Gateway.
11. The BlackBerry Secure Gateway sends the discovery document to the device.
12. The device sends an access token request through the BlackBerry Secure Gateway to the authorization server/identity provider.
13. The authorization server/identity provider sends the access token to the device.
14. When it sends or receives email, the device presents the access token to establish a secure connection to the mail server.

    When the access token expires, the device sends a new token request through the BlackBerry Secure Gateway to the authorization server/identity provider.

Data flow: Sending email from an iOS device using the BlackBerry Secure Gateway

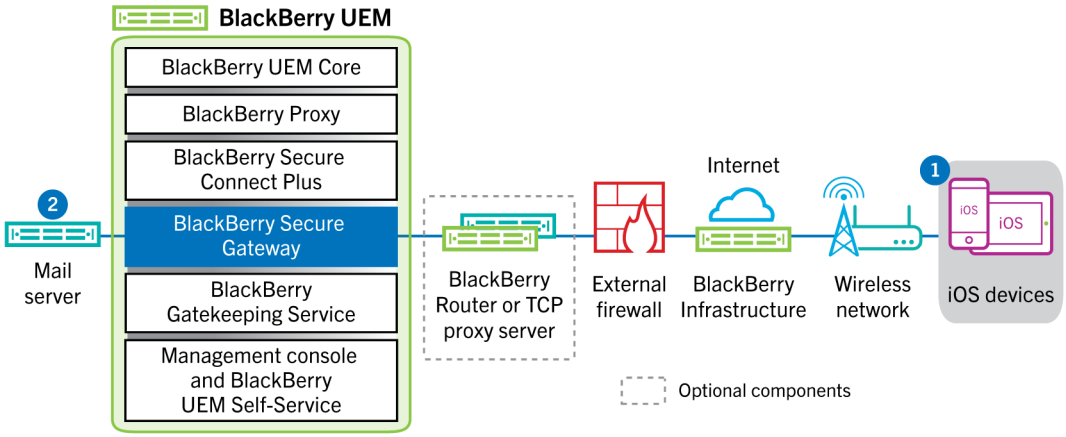
This data flow describes how work email and calendar data travels from iOS devices to the Exchange ActiveSync server using the BlackBerry Secure Gateway.



1. A user creates an email or updates an organizer item in the work space.
2. The device sends the new or changed item through the BlackBerry Infrastructure and the BlackBerry Secure Gateway to the mail server.
3. The mail server updates the organizer data on the user's mailbox or sends the mail item to the recipient and sends a confirmation to the device.

Data flow: Receiving email on an iOS device using the BlackBerry Secure Gateway

This data flow describes how work email and calendar data travels between iOS devices and the Exchange ActiveSync server using the BlackBerry Secure Gateway.

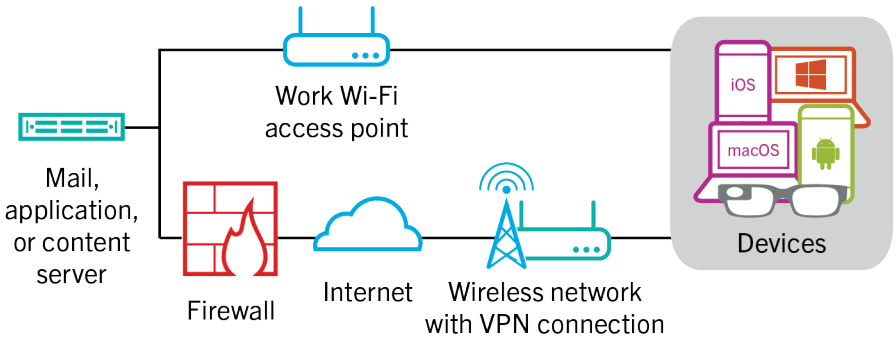


1. The native email client on iOS maintains a permanent connection with the email server over an encrypted and authenticated channel between the BlackBerry Infrastructure and the BlackBerry Secure Gateway and detects changes in the folders configured for synchronization on the mail server.
2. When there are new or changed items for the device, such as a new email message or updated calendar entry, the mail server sends the updates to the device through the secure channel between the BlackBerry Secure Gateway and the BlackBerry Infrastructure to the email or organizer app on the device using the Exchange ActiveSync protocol.

Sending and receiving work data using a VPN or work Wi-Fi network

Devices that have VPN or Wi-Fi profiles configured by you or by the users, may be able to access your organization's resources using your organization's VPN or work Wi-Fi network. To use your organization's VPN, users with an Android device with the MDM controls activation type or Samsung Knox Workspace must manually configure a VPN profile on their devices.

This diagram shows how data can travel when a device connects to your organization's resources using your organization's VPN or work Wi-Fi network.

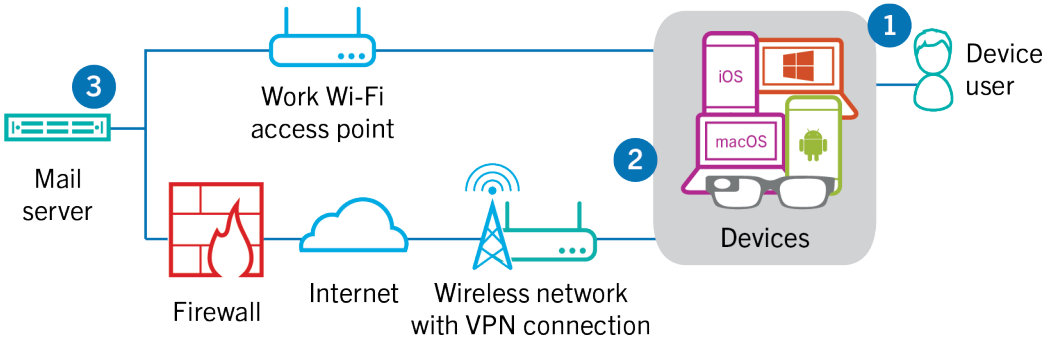


The following table describes when devices use your organization's VPN or work Wi-Fi network to connect to your organization's network.

Device type	Description
Android Enterprise devices and Knox Workspace devices	By default, Android Enterprise and Knox Workspace devices use your organization's VPN or work Wi-Fi network to send and receive work data only when BlackBerry Secure Connect Plus is not enabled.
Windows and macOS devices, and Android devices with the MDM controls activation type	Windows and macOS devices and Android devices with the MDM controls activation type your organization's VPN or work Wi-Fi network to send and receive work data. To use your organization's VPN, Android device users must manually configure a VPN profile on their devices.
iOS	iOS devices use your organization's VPN or work Wi-Fi network to send and receive Exchange ActiveSync data if the BlackBerry Secure Gateway is not enabled. All other work data uses your organization's VPN or work Wi-Fi network.

Data flow: Sending email from a device using a VPN or work Wi-Fi network

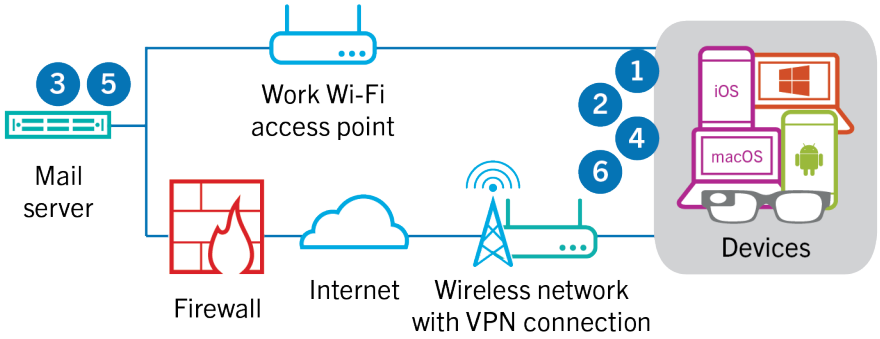
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



1. A user creates an email or updates an organizer item in the work space.
2. The device sends the new or changed item to the mail server over your organization's VPN or work Wi-Fi network.
3. The mail server updates the organizer data on the user's mailbox or sends the mail item to the recipient and sends a confirmation to the device.

Data flow: Receiving email on a device using a VPN or work Wi-Fi network

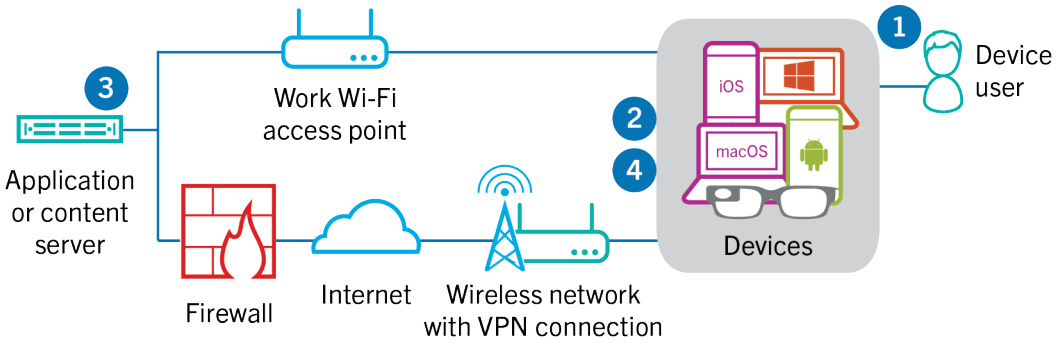
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



1. The device issues an HTTPS request to the mail server and requests that the mail server notify the device when any items change in the folders that are configured to synchronize. The request travels through your organization's VPN or work Wi-Fi network to the mail server.
2. The device stands by.
3. When there are new or changed items for the device, such as a new email or updated calendar entry, the mail server sends the updates to the device. The new or changed items travel through your organization's VPN or work Wi-Fi network to the email or organizer data app on the device.
4. When the synchronization is complete, the device issues another request to restart the process.
5. If there are no new or changed items during this interval, the mail or application server sends a message to the device using the Exchange ActiveSync protocol.
6. The device issues a new request and the process starts over.

Data flow: Accessing an application or content server using a VPN or work Wi-Fi network

This data flow describes how data travels between an application or content server in your organization and an app on a device using a VPN connection or a work Wi-Fi network.



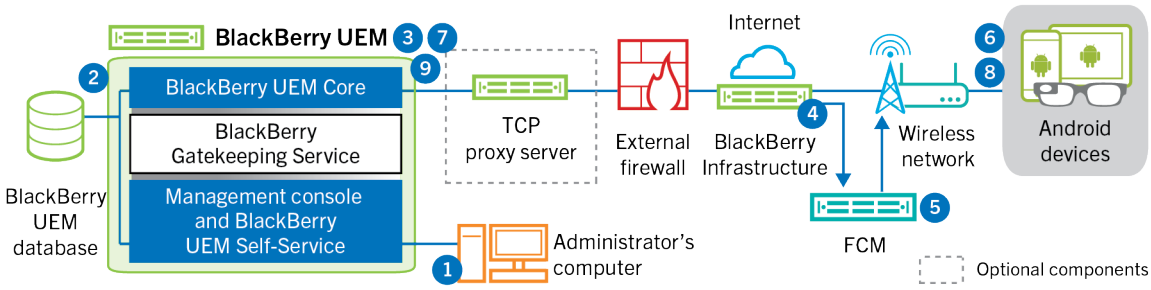
1. The user opens a work app to view work data. For example, the user opens the work browser to navigate the intranet or uses an internally developed app to access your organization's customer data.
2. The app establishes a connection to the application or content server to retrieve the data. The request travels through your VPN or work Wi-Fi network to the application or content server.
3. The application or content server replies with the work data. The work data travels through your VPN or work Wi-Fi network to the app on the work space of the device.
4. The app receives and displays the data on the device.

Data flows: Receiving device configuration updates

When you use the management console to send device commands, such as lock device or delete the work data, or when you perform other device management tasks, such as updates to policy, profile, and app settings or assignments, you trigger a configuration update for the device.

This section provides data flows that detail how data travels through your organization's UEM environment when devices receives configuration updates.

Data flow: Receiving configuration updates on an Android device



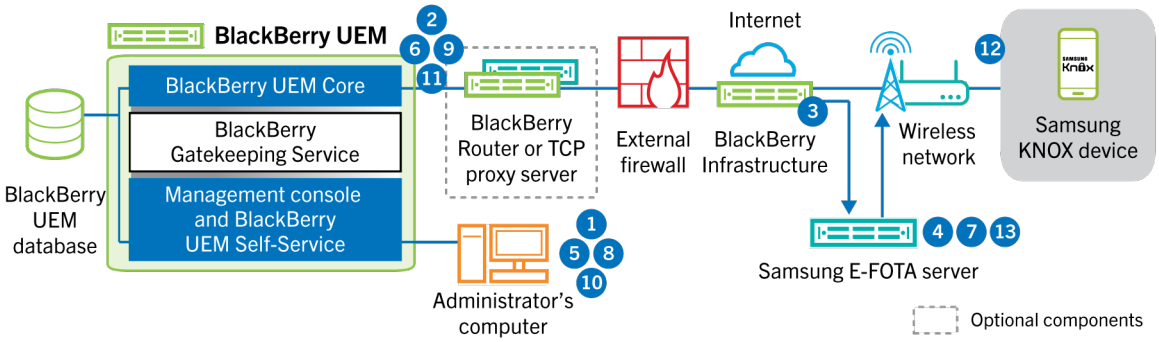
1. An action is taken in the management console that triggers a configuration update for an Android device.
2. Updates are applied in BlackBerry UEM, and objects that must be shared with the device are identified.
3. The BlackBerry UEM Core contacts the BlackBerry Infrastructure, through the BlackBerry Router or TCP proxy server, if installed, and the external firewall over port 3101.
4. The BlackBerry Infrastructure uses the FCM to notify Android devices that an update is pending.
5. The FCM sends a notification to the BlackBerry UEM Client on the Android device to contact the BlackBerry UEM Core.
6. The BlackBerry UEM Client contacts the BlackBerry UEM Core, on port 3101 on the external firewall, to request any pending actions and commands that must be performed on the device.
7. The BlackBerry UEM Core replies, through the BlackBerry Infrastructure and BlackBerry Router or TCP proxy server, if installed, with the highest priority action.

   Priority is given to IT administration commands, such as Delete device data and Lock device, followed by requests for device information, installed apps, and so on. The BlackBerry UEM Core sends only one command at a time. If necessary, additional information is included in the response.
8. The BlackBerry UEM Client inspects the response, schedules the command to be processed, and waits for the command to be run. The BlackBerry UEM Client sends a response to the BlackBerry UEM Core, through the BlackBerry Infrastructure, to update the command status. The status indicates whether the command ran successfully and provides an error message in the event of a failure.
9. If more actions or commands are pending for the device, the BlackBerry UEM Core replies, through the BlackBerry Infrastructure, with the highest priority action. If no actions or commands are pending for the device, the BlackBerry UEM Core replies with an idle command.

   Steps 7 to 9 are repeated until no more pending actions or commands must be performed on the device.

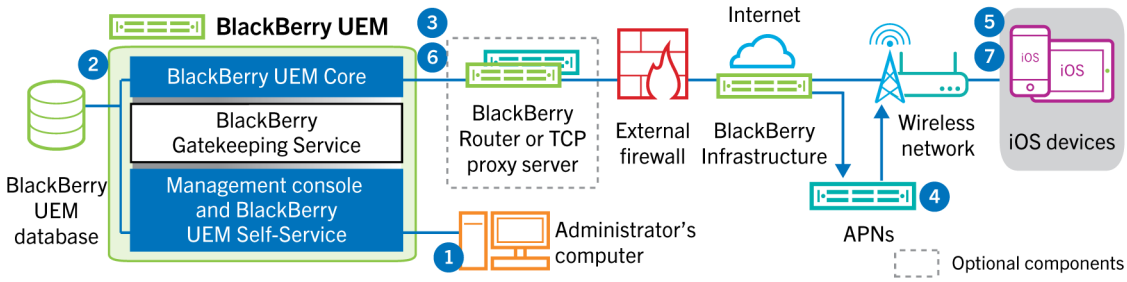
Data flow: Updating firmware on Samsung Knox devices

This data flow describes how data travels when you use Samsung Enterprise Firmware Over the Air to control when firmware updates from Samsung are installed on devices.



1. An administrator adds a Samsung E-FOTA customer ID and license key to BlackBerry UEM.
2. The BlackBerry UEM Core sends the license information to the BlackBerry Infrastructure over a TLS connection.
3. The BlackBerry Infrastructure establishes a TLS connection with the Samsung E-FOTA servers and provides the customer ID and license key.
4. The E-FOTA server verifies the information and returns license information through the BlackBerry Infrastructure to BlackBerry UEM Core.
5. An administrator creates a device SR requirements profile and specifies a Samsung device model, language, and wireless service provider for a new Samsung device firmware rule.
6. The BlackBerry UEM Core connects to the E-FOTA server via the BlackBerry Infrastructure over a TLS connection and sends the specified criteria to the E-FOTA server.
7. The E-FOTA server verifies the criteria and returns firmware information through the BlackBerry Infrastructure to BlackBerry UEM Core.
8. The administrator saves the new device SR requirements profile.
9. The BlackBerry UEM Core connects to the E-FOTA server via the BlackBerry Infrastructure over a TLS connection and sends the profile to the Samsung Cloud.
10. The administrator assigns the device SR requirements profile to one or more users.
11. BlackBerry UEM sends the profile to the BlackBerry UEM Client on the user's Samsung device.
12. The Samsung device registers with the E-FOTA server.
13. If a firmware update is available that meets the parameters specified in the device SR requirements profile, the E-FOTA server sends the update to the device.

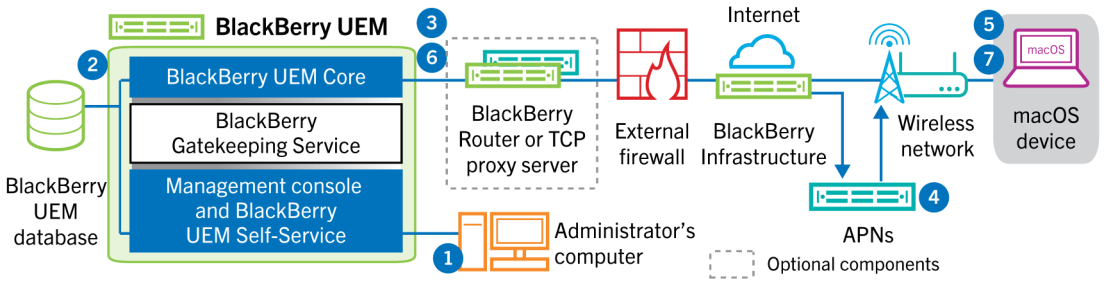
Data flow: Receiving configuration updates on an iOS device



1. An action is taken in the management console that triggers a configuration update for an iOS device. For example, you update the IT policy or assign a new profile or app to the user account.
2. Updates are applied in BlackBerry UEM and objects that must be shared with the device are identified.
3. The BlackBerry UEM Core performs the following actions:
   a. Contacts the BlackBerry Infrastructure, through the BlackBerry Router or TCP proxy server, if installed, and the external firewall over port 3101.
   b. Sends a request through the BlackBerry Infrastructure to the APNs to notify the device that an update is pending.
4. The APNs sends a notification to the native MDM Daemon on the iOS device to contact the BlackBerry UEM Core.
5. When the native MDM Daemon on the iOS device receives the notification, it contacts the BlackBerry UEM Core, on port 3101 on the external firewall, passing through the BlackBerry Router or TCP proxy server, if installed, to retrieve any pending actions.
6. The BlackBerry UEM Core replies with the highest priority action. Priority is given to device actions, such as Delete device data and Lock device. The BlackBerry UEM Core sends only one command at a time. If necessary, additional information is included in the response. If no actions or commands are pending for the device, the BlackBerry UEM Core replies to the device with an idle command.
7. The native MDM Daemon on the iOS device performs the following actions:
   a. Inspects the response from the BlackBerry UEM Core, schedules the command to be processed, and waits for the command to run.
   b. Sends a response to the BlackBerry UEM Core to update the command status. The status indicates whether the command ran successfully and provides an error message in the event of a failure.

   Steps 6 and 7 are repeated until no more pending actions or commands must be performed on the device.

Data flow: Receiving configuration updates on a macOS device



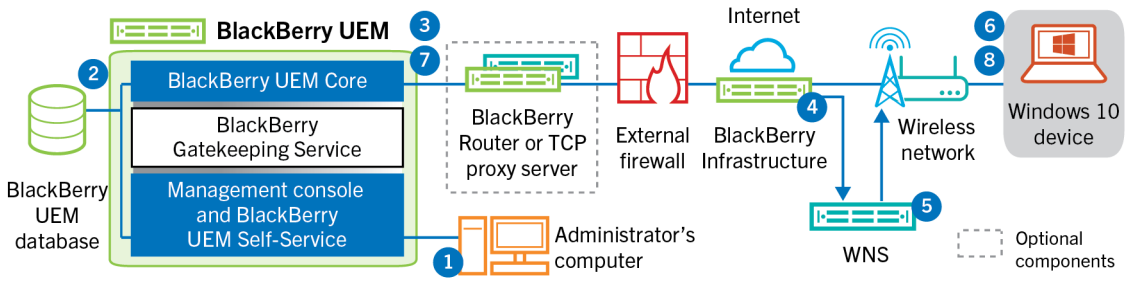
1. An action is taken in the management console that triggers a configuration update for a macOS device. For example, you update the IT policy or assign a new profile or app to the user account.
2. Updates are applied in BlackBerry UEM, and objects that must be shared with the device are identified.
3. The BlackBerry UEM Core performs the following actions:
   a. Contacts the BlackBerry Infrastructure, through the BlackBerry Router or TCP proxy server, if installed, and the external firewall over port 3101.
   b. Sends a request through the BlackBerry Infrastructure to the APNs to notify the device that an update is pending.
4. The APNs sends a notification to the device to contact the BlackBerry UEM Core.
5. When the device receives the notification, it contacts the BlackBerry UEM Core, on port 3101 on the external firewall, passing through the BlackBerry Router or TCP proxy server, if installed, to retrieve any pending actions.

6. When an update is pending for the device, the BlackBerry UEM Core replies with the highest priority action. Priority is given to device actions, such as Delete device data and Lock device. If necessary, additional information is included in the response. If no actions or commands are pending for the device, the BlackBerry UEM Core replies to the device with an empty message.
7. The device performs the following actions:

   a. Inspects the response from the BlackBerry UEM Core, schedules the command to be processed, and waits for the command to run.
   b. Sends a response to the BlackBerry UEM Core to update the command status. The status indicates whether the command ran successfully and provides an error message in the event of a failure.

   Steps 6 and 7 are repeated until no more pending actions or commands must be performed on the device.

Data flow: Receiving configuration updates on a Windows 10 device



1. An action is taken in the management console that triggers a configuration update for a Windows 10 device. For example, you update the IT policy or assign a new profile or app to the user account.
2. Updates are applied in BlackBerry UEM, and objects that must be shared with the device are identified.
3. The BlackBerry UEM Core contacts the BlackBerry Infrastructure, through the BlackBerry Router or TCP proxy server, if installed, and the external firewall over port 3101.
4. The BlackBerry Infrastructure uses the WNS to notify the device that an update is pending.
5. The WNS sends a notification to the device to contact the BlackBerry UEM Core.
6. When the device receives the notification, it contacts the BlackBerry UEM Core, on port 3101 on the external firewall, passing through the BlackBerry Router or TCP proxy server, if installed, to retrieve any pending actions.
7. When an update is pending for the device, the BlackBerry UEM Core replies with the highest priority action. Priority is given to device actions, such as Delete device data and Lock device. If necessary, additional information is included in the response. If no actions or commands are pending for the device, the BlackBerry UEM Core replies to the device with an empty message.
8. The device inspects the response, schedules the command to be processed, and waits for the command to be run. The device sends a response to the BlackBerry UEM Core to update the command status. The status indicates whether the command ran successfully and provides an error message in the event of a failure.

   Steps 7 and 8 are repeated until no more actions or commands are pending for the device.

Legal notice

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