BlackBerry UEM

Architecture and Data Flow Reference

12.14

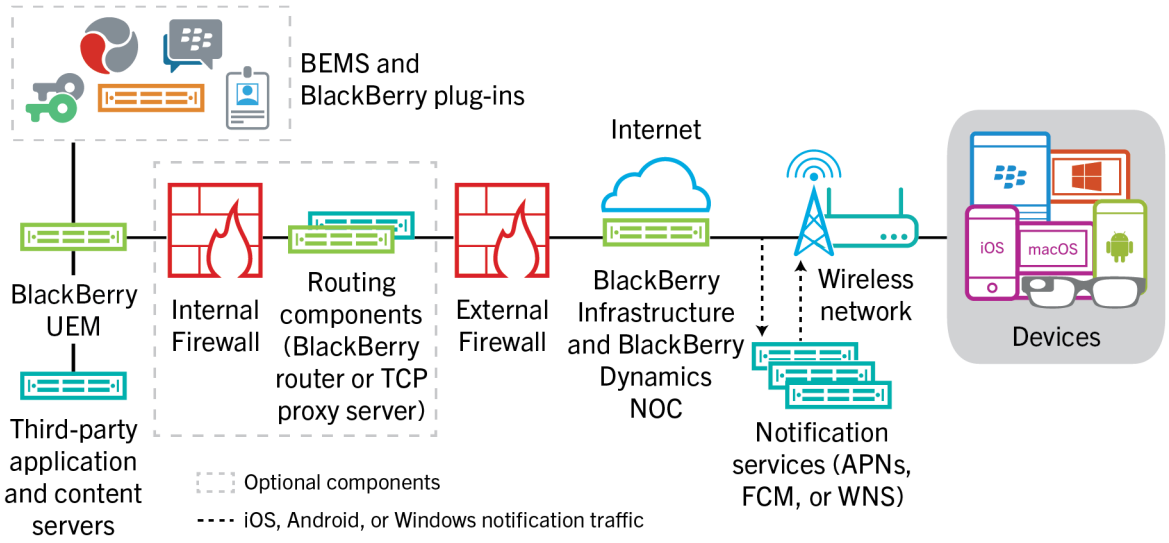
Contents

BlackBerry UEM architecture and data flows

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

The BlackBerry UEM architecture was 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



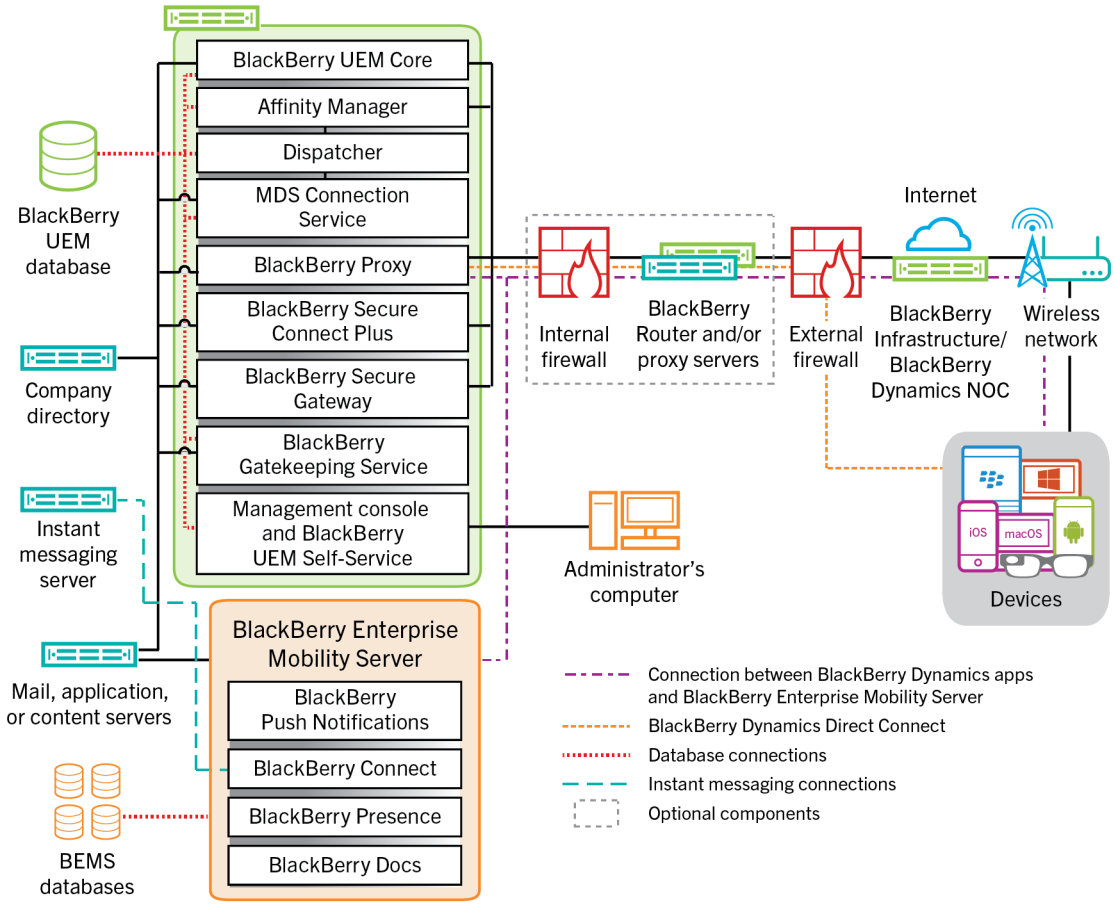
Component	Description
BlackBerry UEM	BlackBerry UEM is a unified endpoint management solution that provides comprehensive multiplatform device, application, and content management with integrated security and connectivity.

Component	Description
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 BlackBerry UEM, the BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM, and provides a trusted path between the organization and every user based on strong, cryptographic, mutual authentication. Because of the end-to-end encryption that protects data transmitted between the device and BlackBerry UEM, BlackBerry UEM maintains a constant connection to the BlackBerry Infrastructure. This ensures 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 BlackBerry 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 and BlackBerry UEM and the BlackBerry Enterprise Mobility Server.
Devices	BlackBerry UEM supports, iOS, macOS, Android, Windows 10, and BlackBerry 10 devices.
Notification services	BlackBerry UEM sends notifications to devices to contact BlackBerry 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, BlackBerry UEM makes a direct connection to the BlackBerry Infrastructure over ports 3101 and 443, and you do not need to install more routing components. However, if your organization's security policy requires 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 BlackBerry 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 requires 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.

Component	Description
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	BlackBerry UEM works with additional BlackBerry enterprise products such as: BlackBerry Enterprise Identity, and BlackBerry 2FA to allow you to extend UEM capabilities in your organization. The BlackBerry Enterprise Mobility Server provides several services used to send work data to and from BlackBerry Dynamics apps.

BlackBerry UEM components

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



For information about the ports used for connections between components, see "Configuring ports" in the Planning content.

Component name	Description
BlackBerry UEM Core	The BlackBerry UEM Core is the central component of the BlackBerry 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.
BlackBerry UEM database	The BlackBerry UEM database is a relational database that contains user account information and configuration information that BlackBerry UEM uses to manage devices and BlackBerry Dynamics apps.

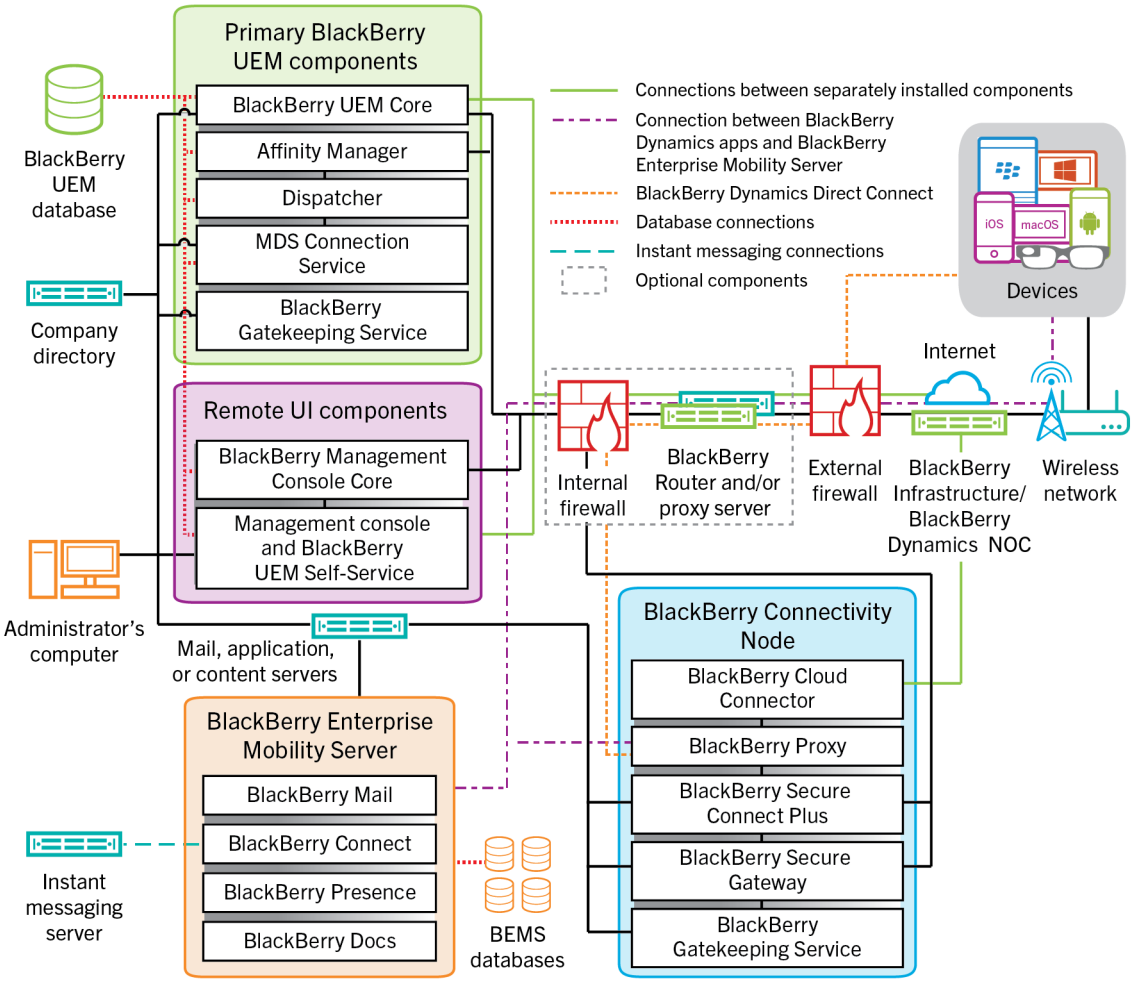
Component name	Description
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service provides a secure connection between BlackBerry 10 devices and your organization's network when the device is not connected to your work Wi-Fi network or using a VPN connection.
BlackBerry Dispatcher	The BlackBerry Dispatcher provides secure connectivity using IPPP for BlackBerry 10 devices.
BlackBerry Affinity Manager	The BlackBerry Affinity Manager is responsible for maintaining an active SRP connection between BlackBerry 10 devices and the BlackBerry Infrastructure when the devices are not using BlackBerry Secure Connect Plus.
BlackBerry Proxy	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	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	The BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and BlackBerry 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 BlackBerry 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 BlackBerry UEM 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 BlackBerry UEM. You use the management console to manage system settings, users, devices, and apps. Users can use BlackBerry UEM Self-Service to set an activation password and send commands to devices, such as set password, lock device, and delete device data.
BlackBerry Enterprise Mobility Server	BEMS consolidates several services used to send work data to and from BlackBerry Dynamics apps, including: BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs.
BlackBerry Enterprise Mobility Server databases	The BEMS databases store user, app, policy, and configuration information.
BlackBerry Push Notifications	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.

Component name	Description
BlackBerry Connect	BlackBerry Connect provides secure instant messaging, company directory look-up, and user presence information to iOS and Android devices.
BlackBerry Presence	BlackBerry Presence provides real-time presence status to BlackBerry Dynamics apps.
BlackBerry Docs	BlackBerry Docs lets your BlackBerry Dynamics app users 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.
BlackBerry Router and/or proxy servers	By default, BlackBerry UEM makes a direct connection to the BlackBerry Infrastructure over ports 3101 and 443. If your organization's security policy requires 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 BlackBerry UEM Core and BlackBerry Proxy support using a third-party HTTP proxy server to connect to the BlackBerry Dynamics NOC.
BlackBerry Infrastructure and BlackBerry Dynamics NOC	The BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM 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 BlackBerry UEM Core, BlackBerry Proxy, and BlackBerry Enterprise Mobility Server.

BlackBerry UEM 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 BlackBerry UEM components.

For more information on the architecture when you install BlackBerry UEM on more than one computer for high availability, see the Planning Guide.



For information about the ports used for connections between components, see "Configuring ports" in the Planning content.

Component name	Description
Primary BlackBerry UEM components	The primary BlackBerry UEM components include the BlackBerry UEM Core and all components installed with it on the same server.

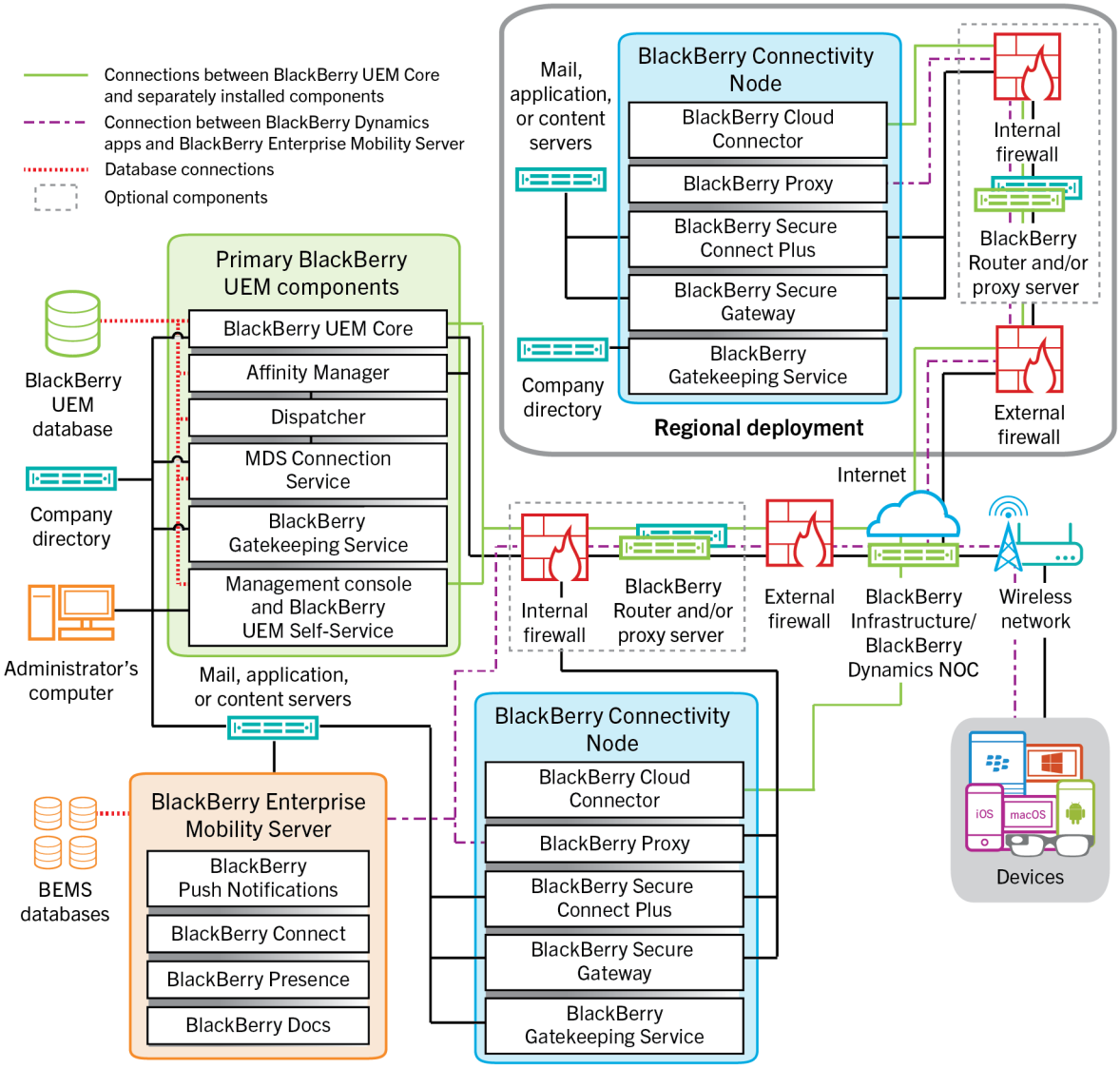
Component name	Description
BlackBerry UEM Core	The BlackBerry UEM Core is the central component of the BlackBerry UEM architecture. It consists of several subcomponents that are responsible for: • Logging, monitoring, reporting, and management functions • Authentication and authorization services • Scheduling and sending commands, IT policies, and profiles to devices • Sending user, policy, and other configuration data to BlackBerry Dynamics apps on devices.
BlackBerry UEM database	The BlackBerry UEM database is a relational database that contains user account information and configuration information that BlackBerry UEM uses to manage devices and BlackBerry Dynamics apps.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service provides a secure connection between BlackBerry 10 devices and your organization's network when the device is not connected to your work Wi-Fi network or using a VPN connection.
BlackBerry Dispatcher	The BlackBerry Dispatcher provides secure connectivity using IPPP for BlackBerry 10 devices.
BlackBerry Affinity Manager	The BlackBerry Affinity Manager is responsible for maintaining an active SRP connection between BlackBerry 10 devices and the BlackBerry Infrastructure when the devices are not using BlackBerry Secure Connect Plus.
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 BlackBerry UEM. Unmanaged devices that try to connect to an organization's mail server can be reviewed, verified, and blocked or allowed through the BlackBerry UEM management console by an administrator.
Remote UI components	The management console and BlackBerry UEM Self-Service can be installed separately from other BlackBerry UEM components. If you install them separately, an instance of the BlackBerry Management Console Core is also installed.
BlackBerry Management Console Core	The BlackBerry Management Console Core handles subtasks specific to administrative activities.
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 BlackBerry UEM. It can be installed separately from other BlackBerry UEM components. You use the management console to manage system settings, users, devices, and apps. Users can access BlackBerry UEM Self-Service to set an activation password and send commands, such as set password, lock device, and delete device data, to devices.

Component name	Description
BlackBerry Connectivity Node	The BlackBerry Connectivity Node installs instances of the BlackBerry UEM device connectivity components to your organization's domain on a different server than the BlackBerry UEM Core. Each BlackBerry Connectivity Node contains these components: • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service
BlackBerry Cloud Connector	The BlackBerry Cloud Connector allows the BlackBerry Connectivity Node components to communicate with the BlackBerry UEM Core. All communication between the BlackBerry Cloud Connector and BlackBerry UEM Core travels through the BlackBerry Infrastructure.
BlackBerry Proxy	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	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	The BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and BlackBerry UEM to your organization's mail server for iOS devices.
BlackBerry Gatekeeping Service (BlackBerry Connectivity Node)	BlackBerry UEM can use instances of BlackBerry Gatekeeping Service that are installed with the BlackBerry Connectivity Node to manage gatekeeping for your mail server. Each instance must be able to access your organization's gatekeeping server. If you want gatekeeping data to be managed only by the BlackBerry Gatekeeping Service that is installed with the primary BlackBerry UEM components, you can disable the BlackBerry Gatekeeping Service in each BlackBerry Connectivity Node
BlackBerry Enterprise Mobility Server	BEMS consolidates several services used to send work data to and from BlackBerry Dynamics apps, including: BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs.
BlackBerry Enterprise Mobility Server databases	The BEMS databases store user, app, policy, and configuration information.

Component name	Description
BlackBerry Infrastructure and BlackBerry Dynamics NOC	The BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM 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 BlackBerry UEM Core, BlackBerry Proxy, and BlackBerry Enterprise Mobility Server.

BlackBerry UEM regional deployment

This diagram shows how the BlackBerry UEM components connect together when one or more instances of the BlackBerry Connectivity Node are installed in a separate location. You can use server groups to specify the regional instance of the BlackBerry Connectivity Node that a device connects to.



For information about the ports used for connections between components, see "Configuring ports" in the Planning content.

Component name	Description
Primary BlackBerry UEM components	The primary BlackBerry UEM components include the BlackBerry UEM Core and all components installed with it on the same server.

Component name	Description
BlackBerry UEM Core	The BlackBerry UEM Core is the central component of the BlackBerry 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.
BlackBerry UEM database	The BlackBerry UEM database is a relational database that contains user account information and configuration information that BlackBerry UEM uses to manage devices and BlackBerry Dynamics apps.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service provides a secure connection between BlackBerry 10 devices and your organization's network when the device is not connected to your work Wi-Fi network or using a VPN connection.
BlackBerry Dispatcher	The BlackBerry Dispatcher provides secure connectivity using IPPP for BlackBerry 10 devices.
BlackBerry Affinity Manager	The BlackBerry Affinity Manager is responsible for maintaining an active SRP connection between BlackBerry 10 devices and the BlackBerry Infrastructure when the devices are not using BlackBerry Secure Connect Plus.
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 BlackBerry UEM. Unmanaged devices that try to connect to an organization's mail server can be reviewed, verified, and blocked or allowed through the BlackBerry UEM management console by an administrator.
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 BlackBerry UEM. It can be installed separately from other BlackBerry UEM components. You use the management console to manage system settings, users, devices, and apps. Users can access BlackBerry UEM Self-Service to set an activation password and send commands, such as set password, lock device, and delete device data, to devices.

Component name	Description
BlackBerry Connectivity Node	The BlackBerry Connectivity Node installs instances of the BlackBerry UEM device connectivity components to your organization's domain on a different server than the BlackBerry UEM Core. Each BlackBerry Connectivity Node contains these components: • BlackBerry Cloud Connector • BlackBerry Proxy • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry Gatekeeping Service If you have regional deployments of the BlackBerry Connectivity Node you must configure the connection between the BlackBerry UEM Core and the server group containing the regional BlackBerry Connectivity Node.
BlackBerry Cloud Connector	The BlackBerry Cloud Connector allows the BlackBerry Connectivity Node components to communicate with the BlackBerry UEM Core. All communication between the BlackBerry Cloud Connector and BlackBerry UEM Core travels through the BlackBerry Infrastructure.
BlackBerry Proxy	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	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	The BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and BlackBerry UEM to your organization's mail server for iOS devices.
BlackBerry Gatekeeping Service (BlackBerry Connectivity Node)	BlackBerry UEM can use instances of BlackBerry Gatekeeping Service installed with the BlackBerry Connectivity Node to manage gatekeeping for your mail server. Each instance must be able to access your organization's gatekeeping server. If you want gatekeeping data to be managed only by the BlackBerry Gatekeeping Service that is installed with the primary BlackBerry UEM components, you can disable the BlackBerry Gatekeeping Service in each BlackBerry Connectivity Node
BlackBerry Enterprise Mobility Server	BEMS consolidates several services used to send work data to and from BlackBerry Dynamics apps, including: BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs.
BlackBerry Enterprise Mobility Server databases	The BEMS databases store user, app, policy, and configuration information.

Component name	Description
BlackBerry Infrastructure and BlackBerry Dynamics NOC	The BlackBerry Infrastructure registers user information for device activation, validates licensing information for BlackBerry UEM 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 BlackBerry UEM Core, BlackBerry Proxy and BlackBerry Enterprise Mobility Server.

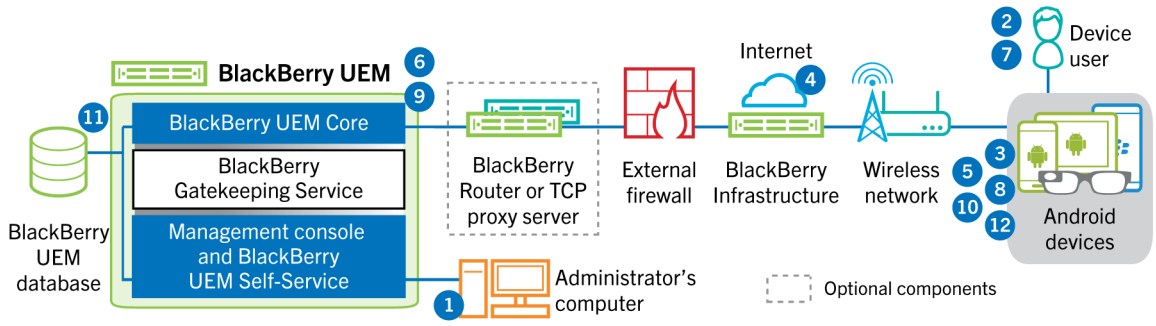
Activating devices and BlackBerry Dynamics apps

When a user activates a device with BlackBerry UEM, the device is associated with BlackBerry 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, see "Device activation" in the Administration content.

Depending on the device type and the activation type that you specify for it, the device and BlackBerry UEM must complete several steps during the activation process to authenticate to each other, secure a communication channel and, if needed, create a work space or encrypt the device before any configuration and work data is sent to the device. For instructions to activate devices, see "Steps to activate devices" in the Administration content.

BlackBerry Dynamics apps provide access to work resources on the device. After BlackBerry Dynamics apps are installed on a device, they must also be activated to allow them to securely access your work resources. For more information about activating BlackBerry Dynamics, see "Generate access keys, activation passwords, or QR codes for BlackBerry Dynamics apps" in the Administration content.

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



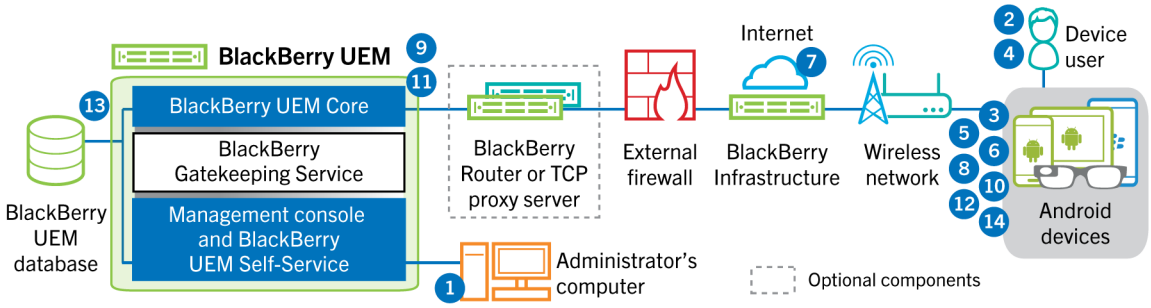
This data flow applies when you allow BlackBerry UEM to manage Google Play accounts. For more information see the Administration content.

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. For more information see the Administration content.

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

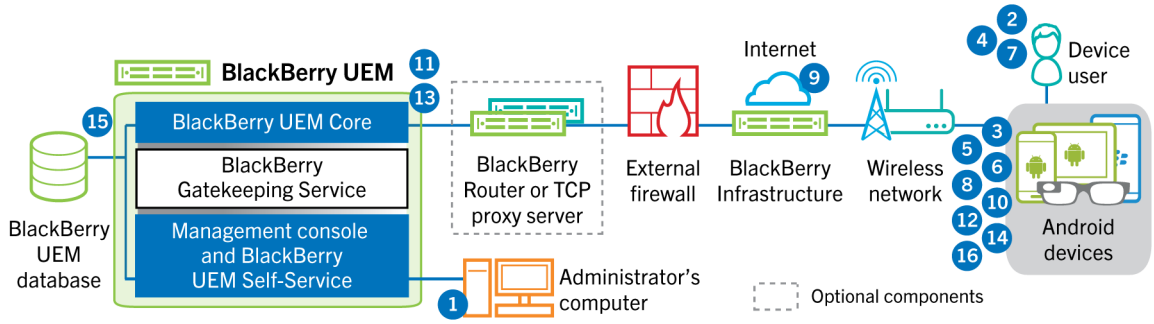
11. BlackBerry UEM performs the following actions:

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. For more information see the Administration content.

1. You perform the following actions:

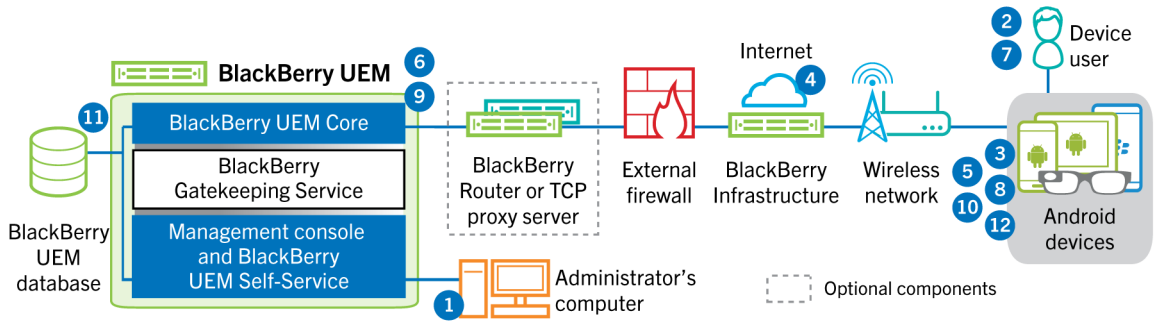
a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company director.
b. Make sure that the "Work space only" activation type is assigned to the user
c. Set the user's activation password

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 `afw#blackberry` instead of their Google user name.
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 G Suite domain. For more information see the Administration content.

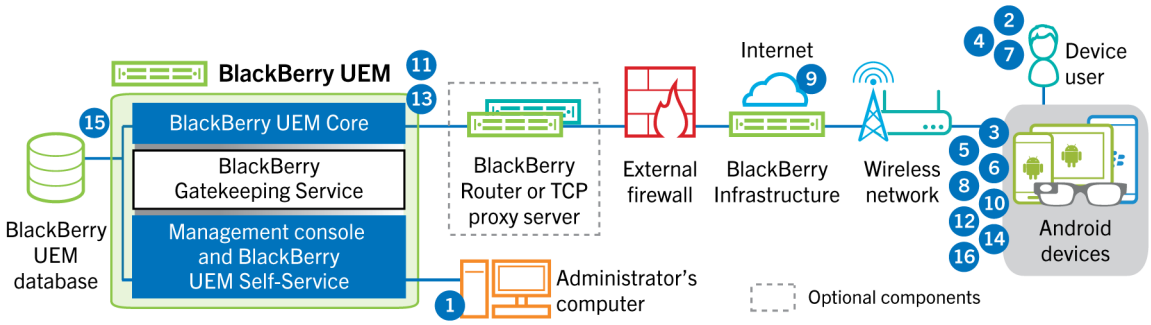
1. You perform the following actions:
   a. Verify that the user has a Google account that is associated with the user's work email address. Optionally, you can configure BlackBerry UEM to create the Google account for the user during the activation process. When BlackBerry UEM creates the account for 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 G Suite domain. For more information see the Administration content.

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.

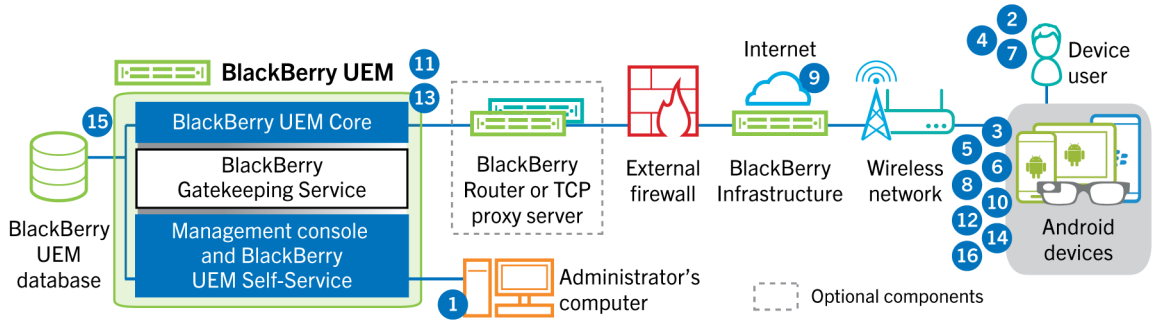
2. The user resets their device to the factory default settings.
3. The device restarts and prompts the user to select a Wi-Fi network and to add an account.
4. The user enters their work email address and password.
5. The device communicates with the Google domain to verify that the user is a work user 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



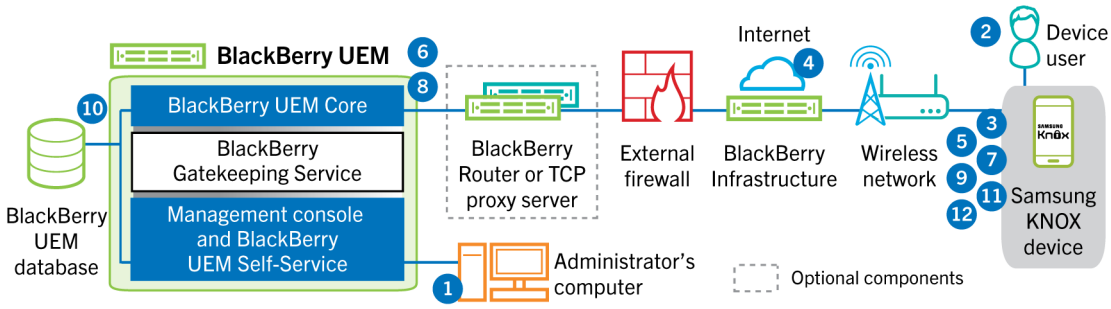
This data flow applies when BlackBerry UEM is connected to a Google Cloud or G Suite domain. For more information see the Administration content.

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

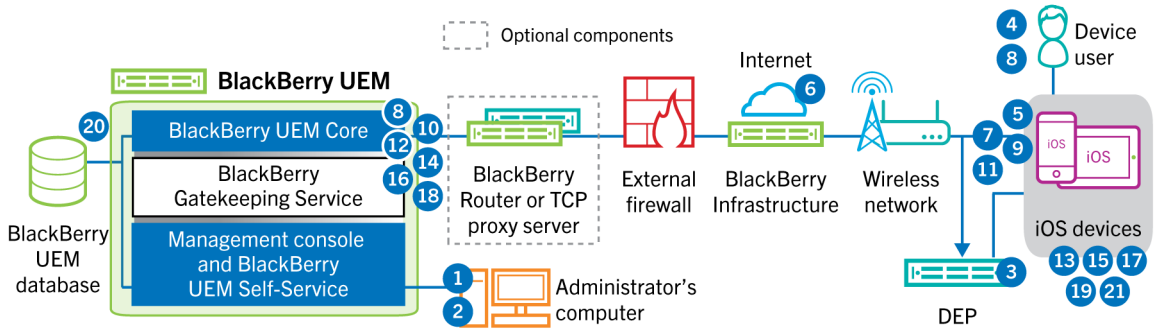
A mutually authenticated TLS session is established between the BlackBerry UEM Client and BlackBerry UEM.

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



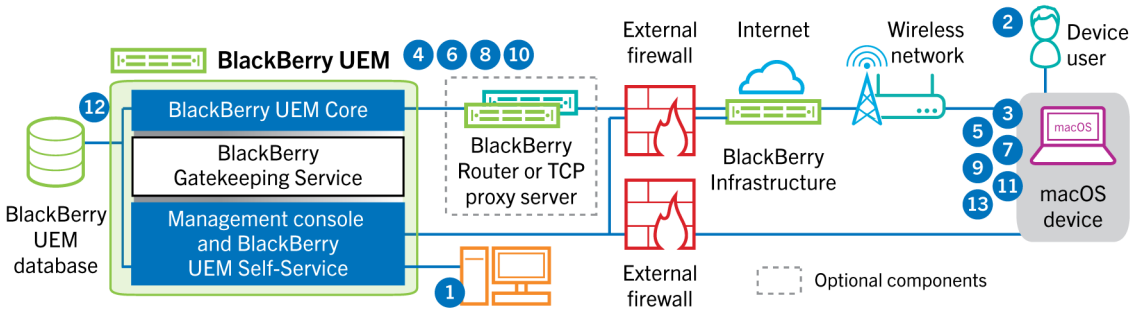
1. If you plan to use the Apple Device Enrollment Program, you perform the following actions:
   a. Make sure that BlackBerry UEM is configured to synchronize with DEP
   b. Register the device in DEP and assign it to an MDM server
   c. Assign an enrollment configuration to the device
2. You perform 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.

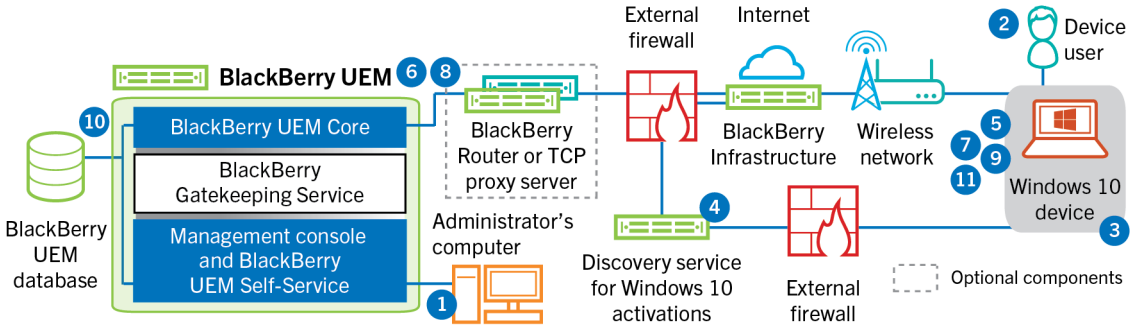
19. The BlackBerry UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
20. BlackBerry UEM stores the device information in the database and sends configuration information to the device.
21. The device sends an acknowledgment to BlackBerry 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

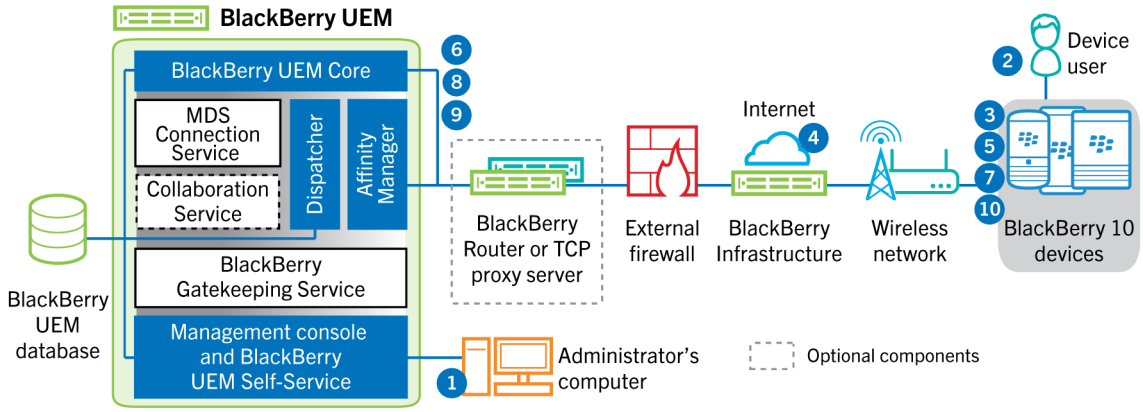


1. You perform the following actions:
   a. Configure the discovery service to simplify Windows 10 activations
   b. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory
   c. Use one of the following options to provide the user with 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 10 device



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. 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 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
2. The user performs the following actions:
   a. Types the username and activation password on the device
   b. For a "Work and personal - Regulated" or "Work space only" activation, accepts the organization notice, which outlines the terms and conditions that the user must agree to
3. If the activation is a "Work space only" activation, the device deletes all existing data and restarts. For other activation types, the Enterprise Management Agent 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 Enterprise Management Agent
5. The device performs the following actions:
   a. Establishes a connection with BlackBerry UEM
   b. Generates a shared symmetric key that is used to protect the CSR and response BlackBerry UEM using the activation password and EC-SPEKE.
   c. Creates an encrypted CSR and HMAC as follows:
      - Generates a key pair for the certificate
      - Creates a PKCS#10 CSR that includes the public key of the key pair
      - Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS#5 padding

- Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR

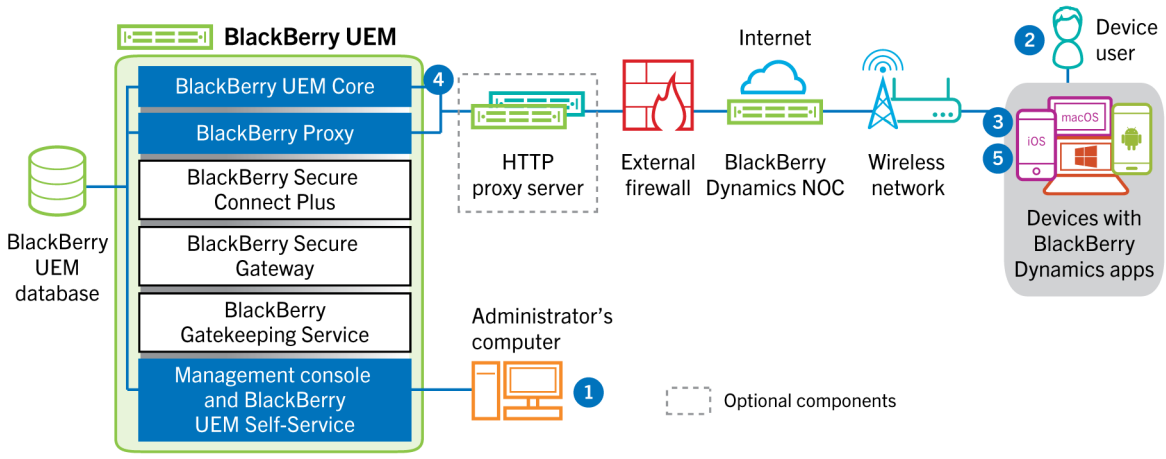
d. Sends the encrypted CSR and HMAC to BlackBerry UEM

6. BlackBerry UEM performs the following actions:
   a. Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
   b. Retrieves the username, work space ID, and your organization's name from the BlackBerry UEM database
   c. Packages a client certificate using the information it retrieved and the CSR that the device sent
   d. Signs the client certificate using the enterprise management root certificate
   e. Encrypts the client certificate, enterprise management root certificate, and the BlackBerry UEM URL using the shared symmetric key and AES-256 in CBC mode with PKCS#5 padding
   f. Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the BlackBerry UEM URL and appends it to the encrypted data
   g. Sends the encrypted data and HMAC to the device
7. The device performs the following actions:
   a. Verifies the HMAC
   b. Decrypts the data it received from BlackBerry UEM
   c. Stores the client certificate and the enterprise management root certificate in its keystore
8. BlackBerry UEM performs the following actions:
   a. BlackBerry UEM Core assigns the new device to a BlackBerry UEM instance in the domain
   b. BlackBerry UEM Core notifies the active BlackBerry Affinity Manager that a new device is assigned to the BlackBerry UEM instance
   c. The active BlackBerry Affinity Manager notifies the BlackBerry Dispatcher on that BlackBerry UEM instance that there is a new device
   d. The BlackBerry UEM Core sends configuration information, including enterprise connectivity settings to the device
9. BlackBerry UEM Core and the device generate the device transport key using ECMQV and the authenticated long-term public keys from the client certificate and the server certificate for BlackBerry UEM. This key is used to encrypt work data when not using BlackBerry Secure Connect Plus and push to IPPP data.
10. The device sends an acknowledgment over TLS to BlackBerry UEM to confirm that it received and applied the IT policy and other data and created the work space. The activation process is complete.

The elliptic curve protocols used during the activation process use the NIST-recommended 521-bit curve.

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.

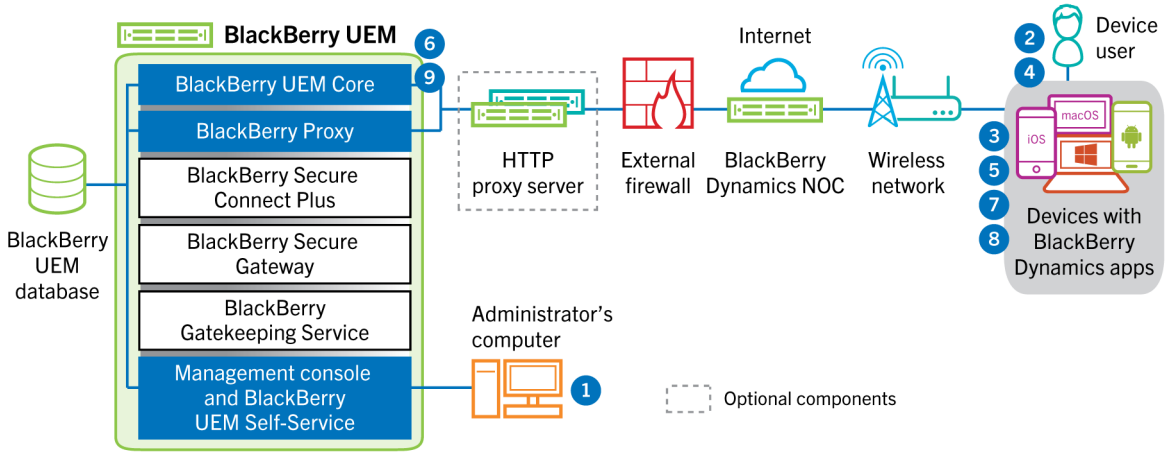


1. An administrator performs the following actions:
   a. Assigns one or more BlackBerry Dynamics apps to a user.
   b. Issues activation credentials (access key, activation password, or QR code) and sends them to the user or instructs the user to generate credentials from BlackBerry UEM Self-Service.
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.

Sending and receiving work data

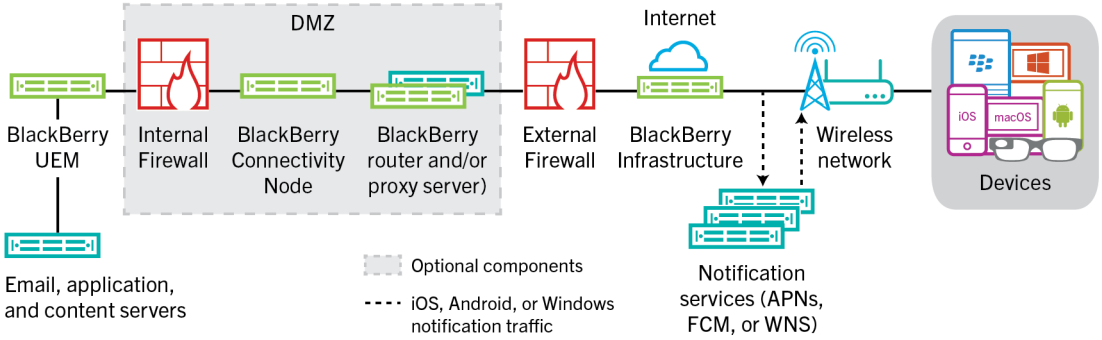
When devices that are active on BlackBerry UEM send and receive work data, they connect to your organization's mail, application, or content servers. For example, when they use the work email or calendar apps, devices establish a connection to your organization's mail server. When they use the work browser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

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 BlackBerry 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 BlackBerry 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.
BlackBerry 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 BlackBerry 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 BlackBerry UEM. If you use the BlackBerry Secure Gateway, you don't have to expose your mail server outside of the firewall to allow users with iOS devices to connect to Microsoft Exchange when they are not connected to your VPN or work Wi-Fi network. • For BlackBerry 10, 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. • BlackBerry 10 devices can use enterprise connectivity for all work data. Enterprise connectivity encrypts and authenticates all work data and sends it through BlackBerry 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.



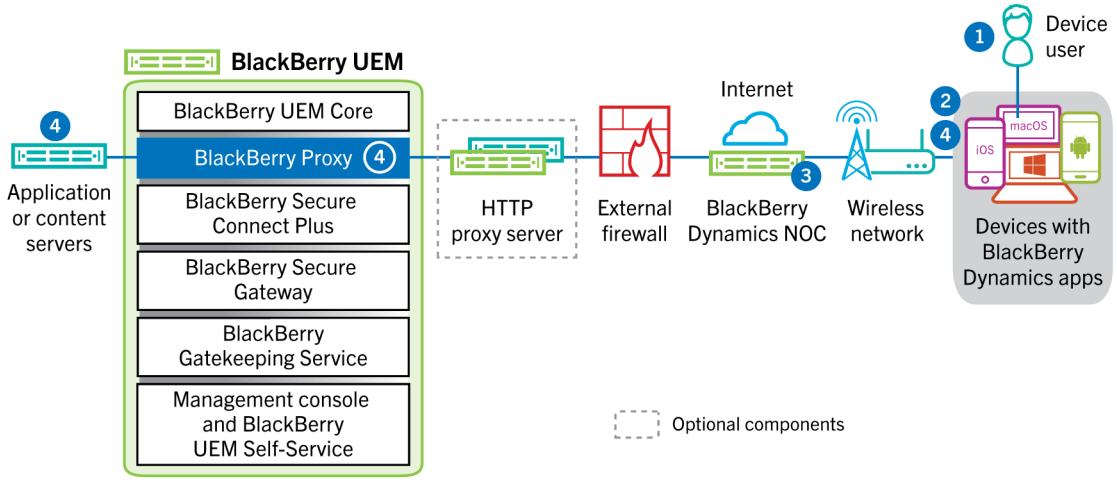
The following table lists the circumstances when devices connect to BlackBerry UEM and your organization's network through the BlackBerry Infrastructure.

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 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, Samsung Knox Workspace, and BlackBerry 10 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 and BlackBerry 10 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.
BlackBerry 10 devices	BlackBerry 10 devices use this communication path to send and receive work data when this is the most direct, cost-efficient route available.

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.

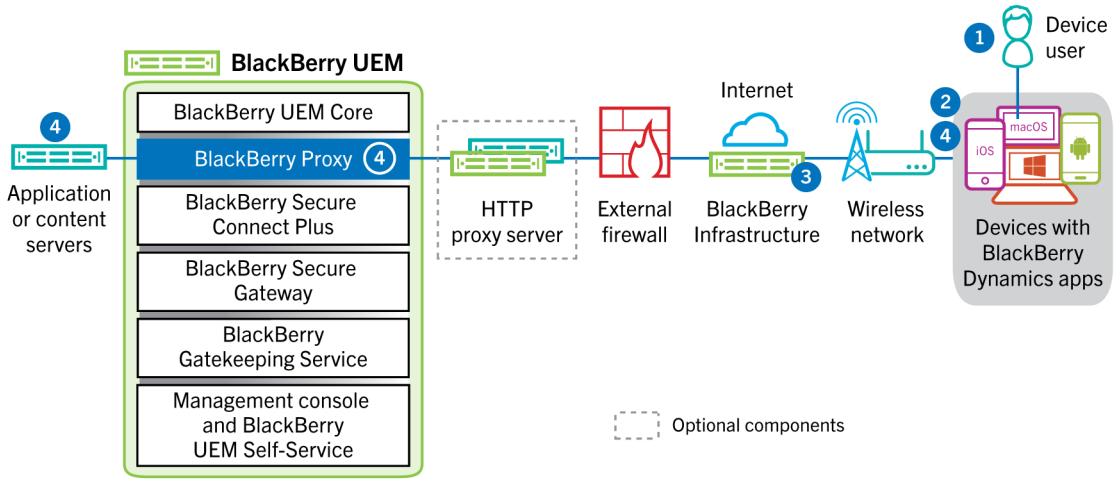


1. The user opens a BlackBerry Dynamics app to access work data.
2. The BlackBerry Dynamics app establishes a connection to the BlackBerry Dynamics NOC. The connection is authenticated with the master link key that was created when the app was activated.
3. The BlackBerry Dynamics NOC communicates with 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.

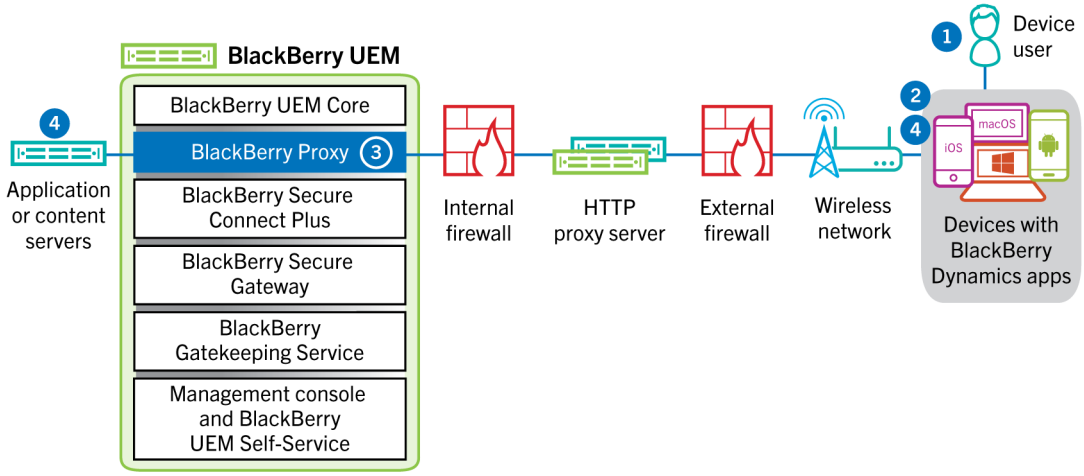
This data flow describes how data travels when a BlackBerry Dynamics app accesses an application or content server in your organization through the BlackBerry Infrastructure and BlackBerry UEM.



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.



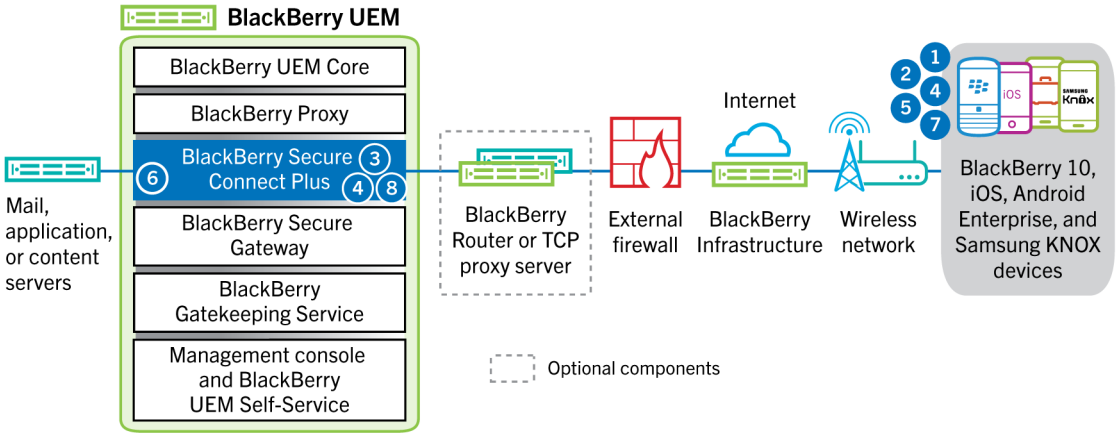
1. The user opens a BlackBerry Dynamics app to access work data.
2. The BlackBerry Dynamics app establishes a TLS connection to BlackBerry Proxy.
3. BlackBerry Proxy authenticates with the BlackBerry Dynamics app. BlackBerry Proxy authenticates with the app using its server certificate. BlackBerry Proxy 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



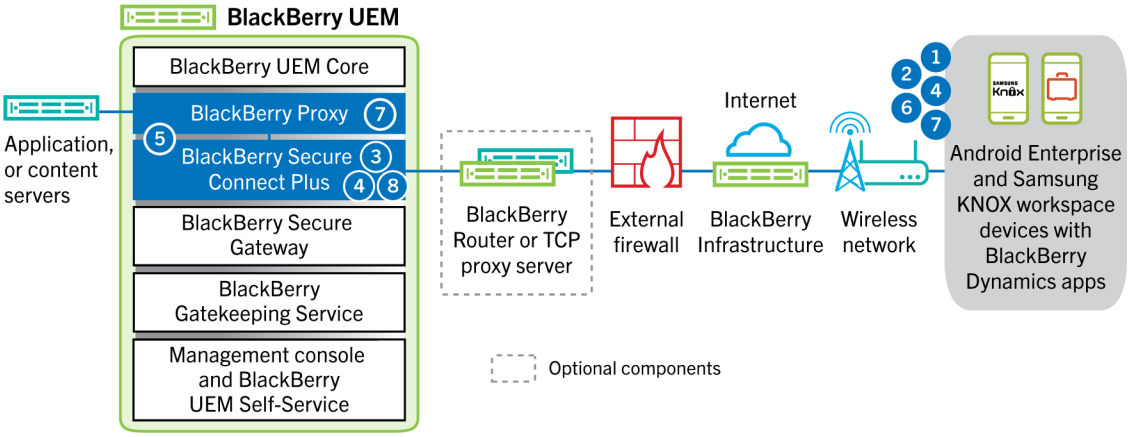
1. The user opens an app to access work data from a content or application server behind your organization's firewall.
   - For Android Enterprise devices, all work space apps except those you choose to restrict use BlackBerry Secure Connect Plus.
   - For Samsung Knox Workspace devices, you specify 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.
   - For BlackBerry 10 devices and Android Enterprise devices, all work space 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.

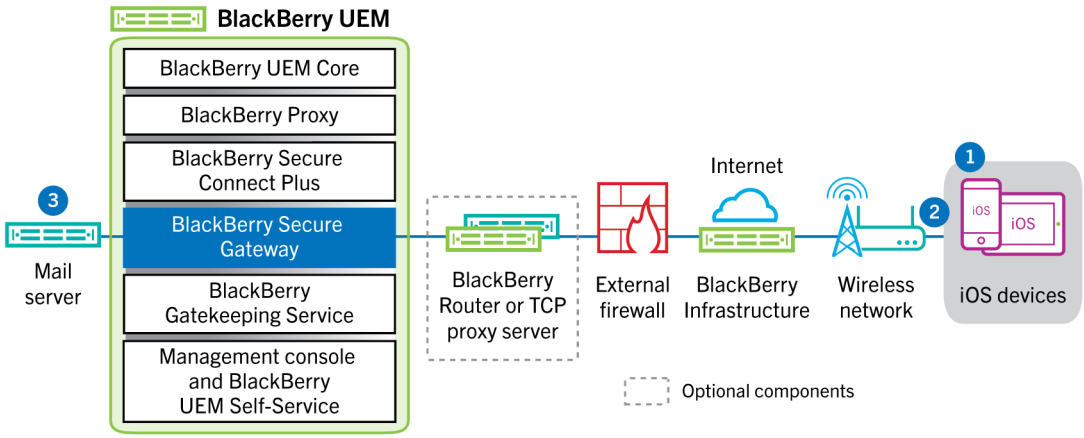
If you are using BlackBerry Secure Connect Plus with BlackBerry Dynamics apps on an Android Enterprise device or a Samsung Knox Workspace device, it is recommended that you configure BlackBerry UEM not to send BlackBerry Dynamics app data through the BlackBerry Dynamics NOC to reduce network latency.



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

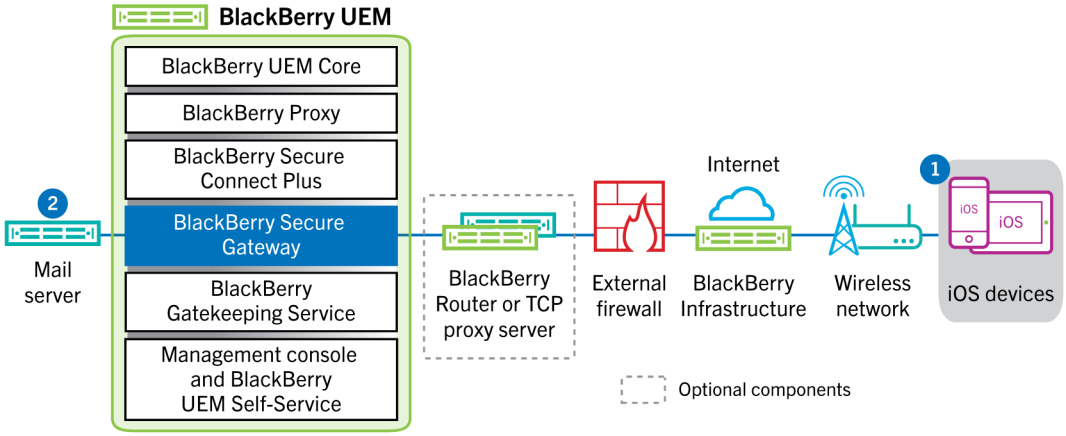
This data flow describes how work email and calendar data travels from iOS devices to the Exchange ActiveSync server using the BlackBerry Secure Gateway.



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

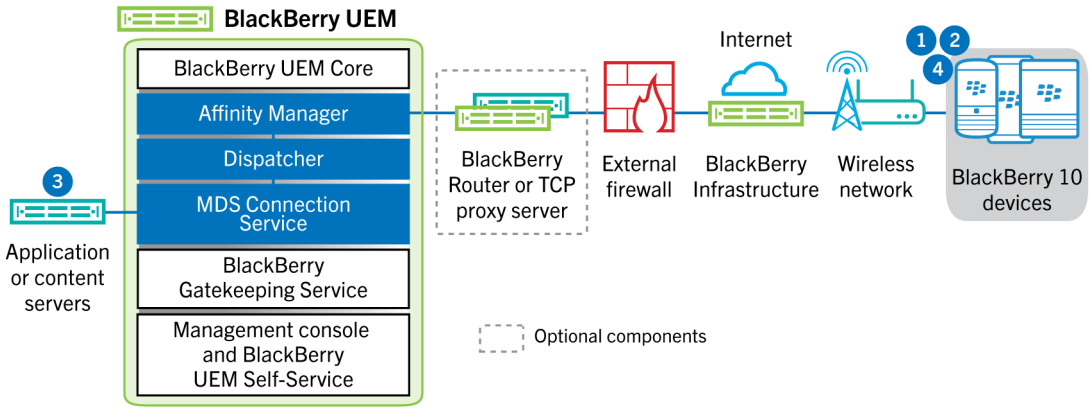
This data flow describes how work email and calendar data travels between iOS devices and the Exchange ActiveSync server using the BlackBerry Secure Gateway.



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.

Data flow: Accessing an application or content server from a BlackBerry 10 device

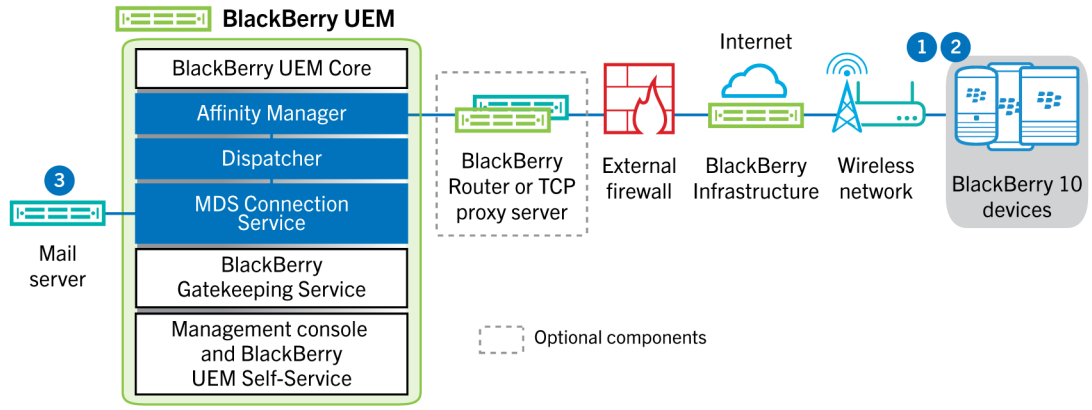
This data flow describes how data travels when a work app on a BlackBerry 10 device accesses an application or content server in your organization when BlackBerry Secure Connect Plus is not enabled.



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 BlackBerry Work Drives to access a file on a network drive.
2. The app establishes a connection to the application or content server to retrieve the data. The request travels through the BlackBerry Infrastructure, BlackBerry Affinity Manager, BlackBerry Dispatcher, and BlackBerry MDS Connection Service to the application or content server.
3. The application or content server replies with the work data. The work data travels through the BlackBerry MDS Connection Service, BlackBerry Dispatcher, BlackBerry Affinity Manager, and BlackBerry Infrastructure to device.
4. The app receives and displays the data on the device.

Data flow: Sending email from a BlackBerry 10 device

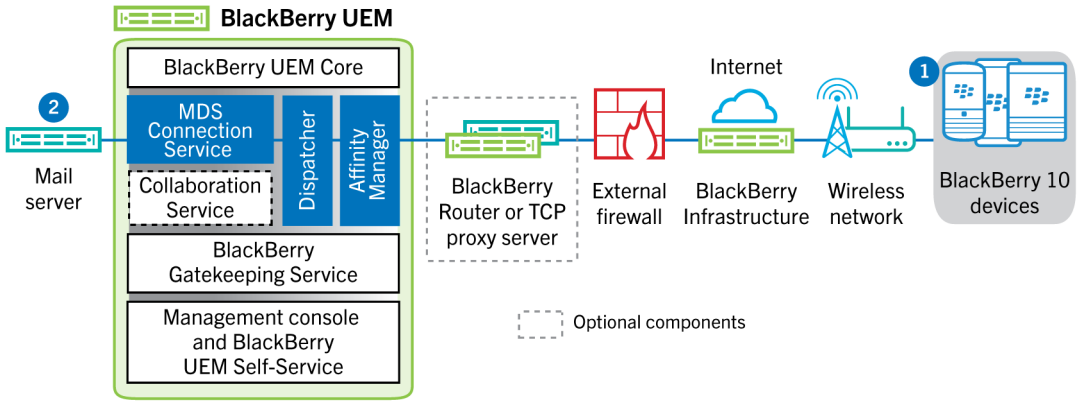
This data flow describes how work email and calendar data travels from BlackBerry 10 devices to the Exchange ActiveSync server when BlackBerry Secure Connect Plus in not enabled.



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, BlackBerry Affinity Manager, BlackBerry Dispatcher, and BlackBerry MDS Connection Service 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 a BlackBerry 10 device

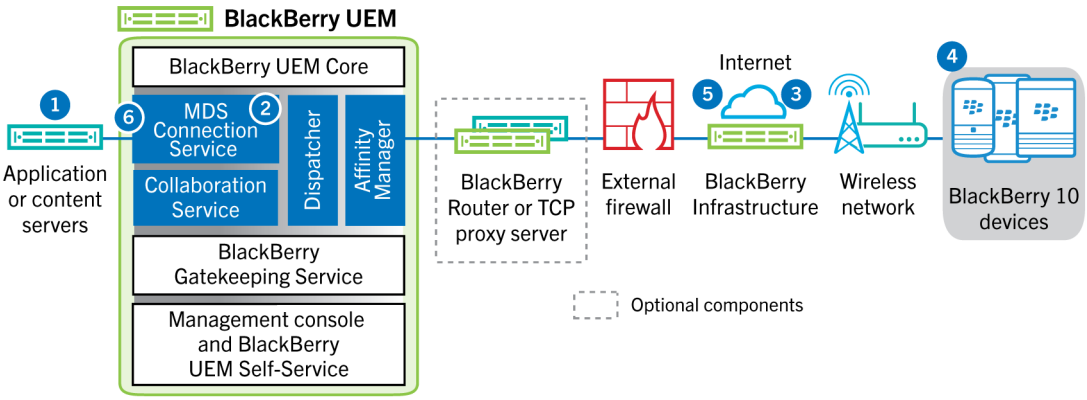
This data flow describes how work email messages are received from the Exchange ActiveSync server on BlackBerry 10 devices when BlackBerry Secure Connect Plus is not enabled.



1. The native email client on the device maintains a permanent connection with the email server over an encrypted and authenticated channel through the BlackBerry Infrastructure, BlackBerry Affinity Manager, BlackBerry Dispatcher, and BlackBerry MDS Connection Service 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 BlackBerry MDS Connection Service, BlackBerry Dispatcher, BlackBerry Affinity Manager, and BlackBerry Infrastructure to the email or organizer app on the device using the Exchange ActiveSync protocol.

Data flow: Receiving enterprise push updates on a BlackBerry 10 device

This data flow describes how work data travels from an application server to an appropriate app in the work space of a BlackBerry 10 device when BlackBerry Secure Connect Plus is not enabled.

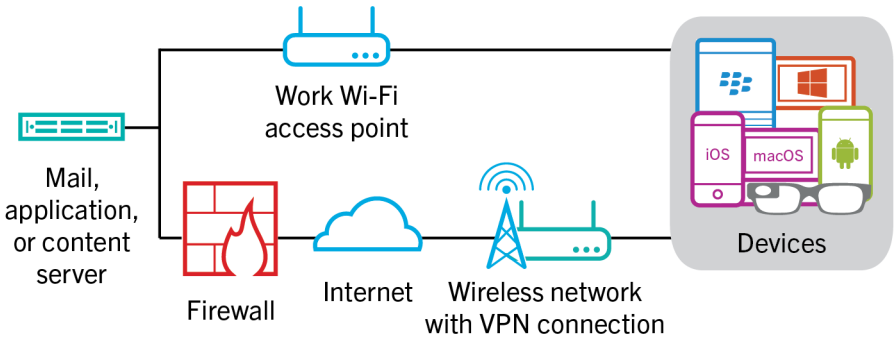


1. When there is new or updated data for a work app on a BlackBerry 10 device, the application or content server pushes the data to the BlackBerry MDS Connection Service using an HTTP or HTTPS request.
2. The BlackBerry MDS Connection Service sends the pushed data through the BlackBerry Dispatcher, BlackBerry Affinity Manager, and BlackBerry Infrastructure over port 3101 on the firewall.
3. The BlackBerry Infrastructure sends the data to the BlackBerry 10 device.
4. The BlackBerry 10 device sends a delivery confirmation to the BlackBerry Infrastructure. The device app detects the incoming content and displays the content when the user opens the app.
5. The BlackBerry Infrastructure sends a delivery confirmation through the BlackBerry Affinity Manager and the BlackBerry Dispatcher to the BlackBerry MDS Connection Service.
6. If configured to do so, the BlackBerry MDS Connection Service sends the delivery confirmation to the push initiator using an HTTP request.

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.

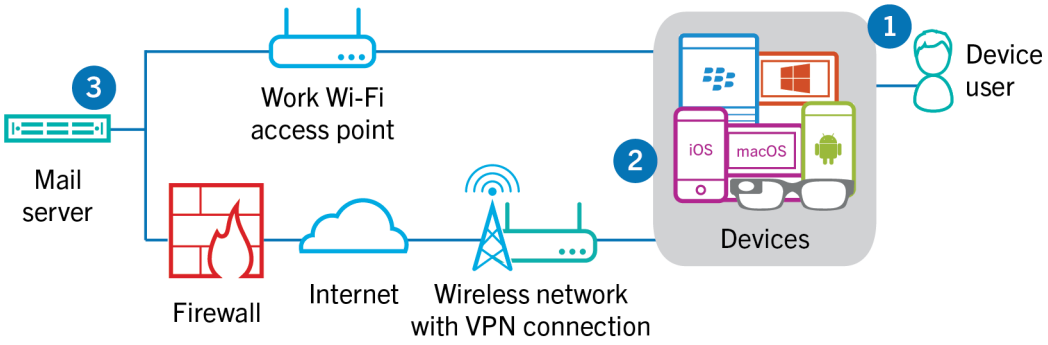


The following table describes when devices use your organization's VPN or work Wi-Fi network to connect to your organization's network.

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.
BlackBerry 10	BlackBerry 10 devices use your organization's VPN or work Wi-Fi network to send and receive work data when this is the most direct, cost-efficient route available. BlackBerry 10 devices use only VPN and Wi-Fi profiles configured by you, not by the user, when accessing work data.

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

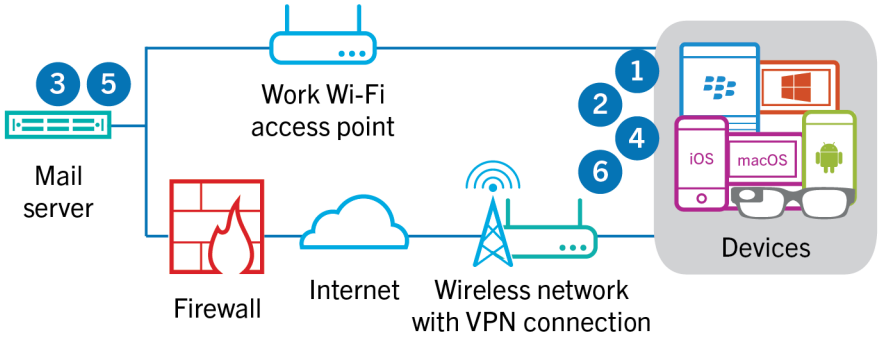
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



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

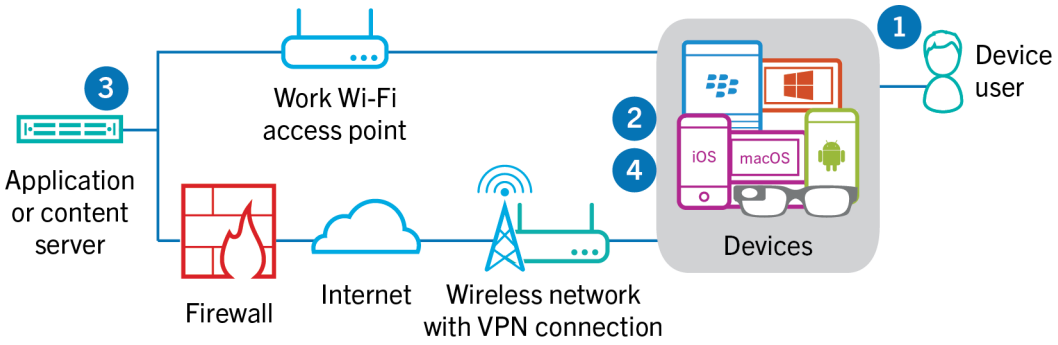
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



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.

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.

When a configuration update needs to be sent to a device, BlackBerry UEM notifies the device that a configuration update is pending. Devices also poll BlackBerry UEM regularly to ask for any actions that need to be run on the device to prevent any configuration update from being missed if a notification is not received on the device.

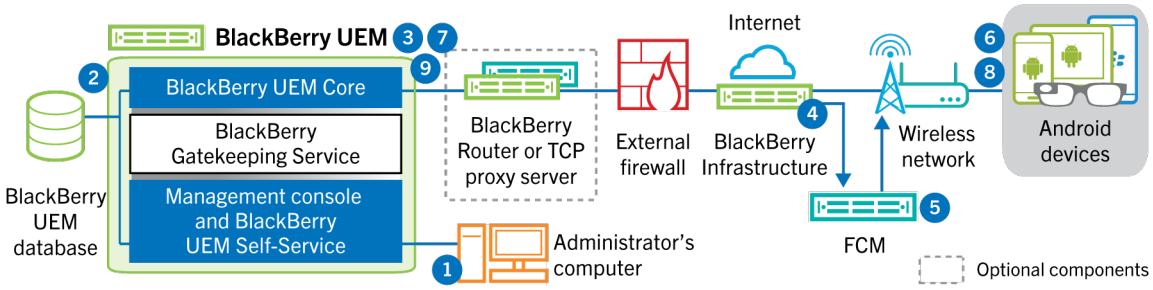
On Android devices, the BlackBerry UEM Client receives and completes all configuration updates.

On iOS devices, the BlackBerry UEM Client app displays compliance status and configuration information for the device, such as apps or policies assigned to it. However, the native MDM Daemon on the device receives and completes all configuration updates sent to the device.

On Windows 10 and macOS devices, which do not require the BlackBerry UEM Client for activation, the native MDM Daemon receives and completes all configuration updates sent to the device.

On BlackBerry 10 devices, the Enterprise Management Agent receives and completes all configuration updates.

Data flow: Receiving configuration updates on an Android device



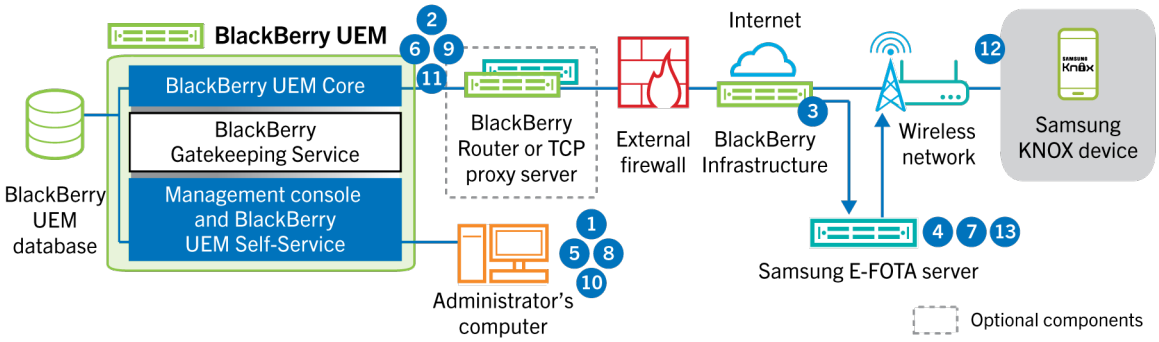
1. An action is taken in the management console that triggers a configuration update for an Android device.
2. Updates are applied in BlackBerry UEM, and objects that must be shared with the device are identified.
3. The BlackBerry UEM Core contacts the BlackBerry Infrastructure, through the BlackBerry 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 GCM 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.

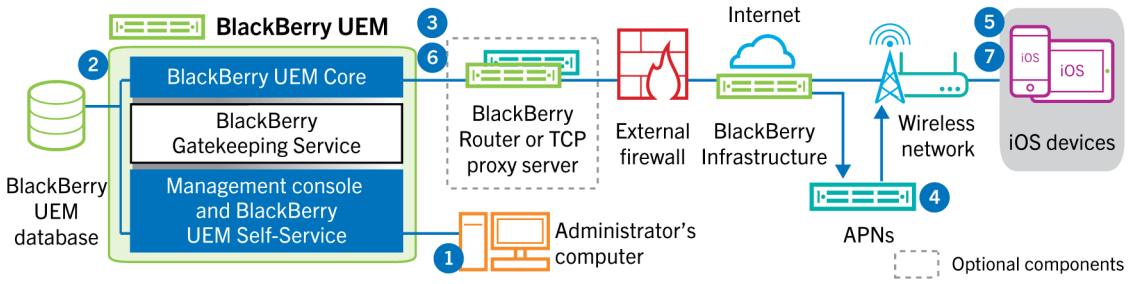
Data flow: Updating firmware on Samsung Knox devices

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. For more information, see Controlling the software releases that are installed on devices in the Administration content.



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.

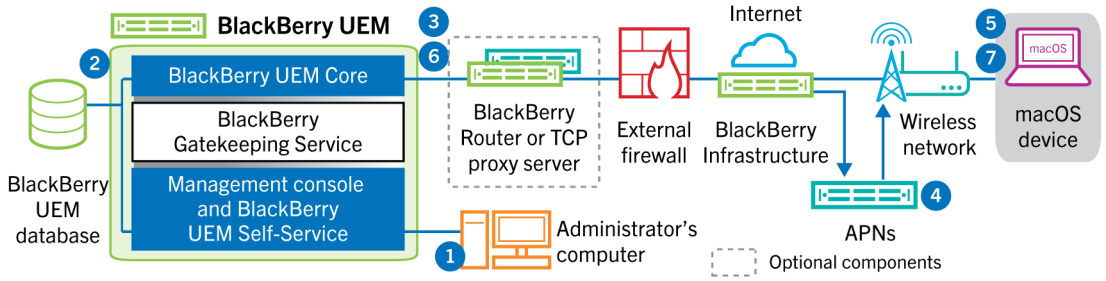
Data flow: Receiving configuration updates on an iOS device



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.

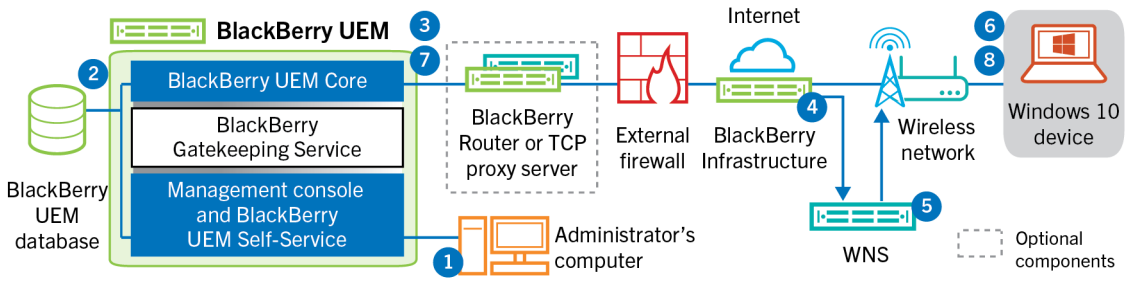
Data flow: Receiving configuration updates on a macOS device



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

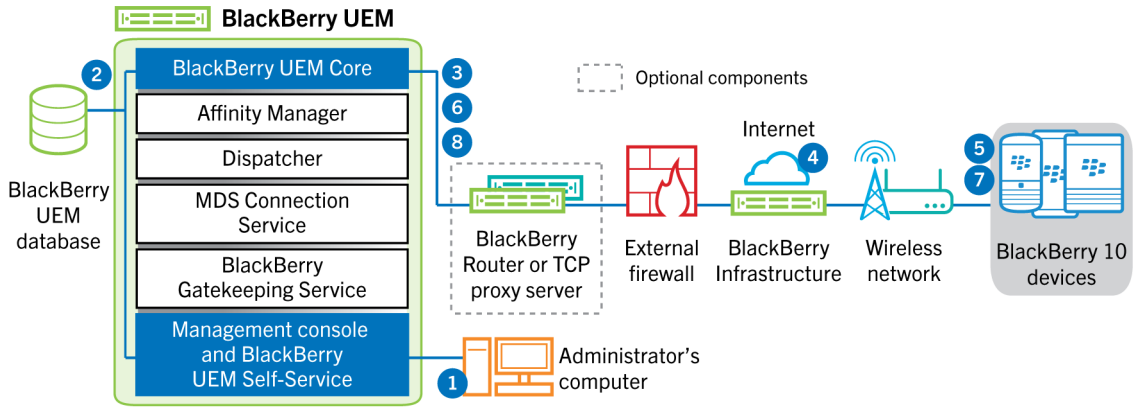


1. An action is taken in the management console that triggers a configuration update for a Windows 10 device. For example, you update the IT policy or assign a new profile or app to the user account.
2. Updates are applied in BlackBerry UEM, and objects that must be shared with the device are identified.
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.

Data flow: Receiving configuration updates on a BlackBerry 10 device



1. An action is taken in the management console that triggers a configuration update for the 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 notifies the BlackBerry Infrastructure that there is an update for a device. The notification passes through the BlackBerry Router or TCP proxy server, if installed, and the external firewall, over port 3101.
4. The BlackBerry Infrastructure notifies the Enterprise Management Agent on the device that there is an update.
5. The Enterprise Management Agent on the device polls the BlackBerry UEM Core to request any pending actions and commands that must be performed on the device. This poll passes through the BlackBerry Infrastructure and the BlackBerry Router, if installed, to the BlackBerry UEM Core.
6. 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.
7. The Enterprise Management Agent on the device receives the configuration updates and applies the new or updated configuration on the device. The Enterprise Management Agent 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.
8. 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 6 to 8 are repeated until no more pending actions or commands must be performed on 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