



# **BlackBerry UEM Cloud**

## **Architecture and Data Flows**

12.18



# Contents

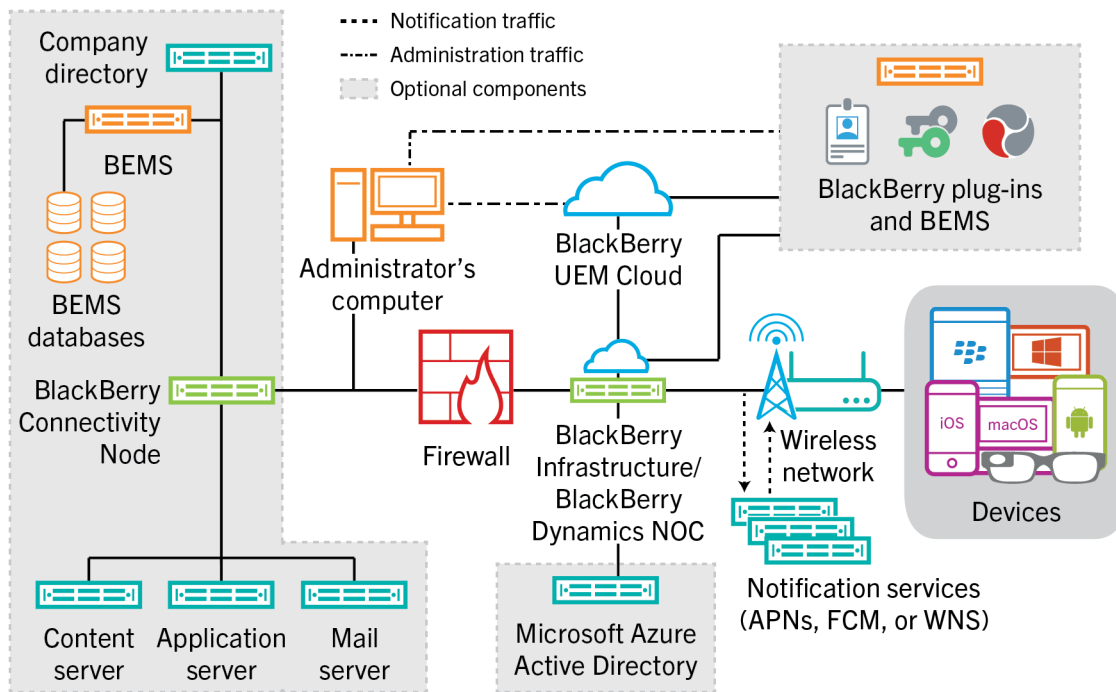
- BlackBerry UEM Cloud architecture and data flows..... 4**
  - Architecture: BlackBerry UEM Cloud solution..... 4
  
- Activating devices and BlackBerry Dynamics apps..... 7**
  - Data flow: Activating an iOS, Android, or Windows 10 device..... 7
  - Data flow: Activating a macOS device..... 9
  - Data flow: Activating a BlackBerry Dynamics app for the first time on a device..... 10
  - Data flow: Activating a BlackBerry Dynamics app when one is already activated on the device..... 11
  
- Data flow: Receiving configuration updates on a device..... 12**
  
- Sending and receiving work data..... 13**
  - Sending and receiving work data using BlackBerry UEM Cloud and the BlackBerry Infrastructure..... 15
    - Data flow: Sending email from an iOS device using the BlackBerry Secure Gateway..... 16
    - Data flow: Receiving email on an iOS device using the BlackBerry Secure Gateway..... 16
    - Data flow: Sending and receiving work data using BlackBerry Secure Connect Plus..... 17
    - Data flow: Sending and receiving work data from a BlackBerry Dynamics app on an Android device using BlackBerry Secure Connect Plus..... 17
    - Data flow: Sending and receiving work data from a BlackBerry Dynamics app..... 18
    - Data flow: Sending and receiving work data from a BlackBerry Dynamics app using BlackBerry Dynamics Direct Connect..... 19
  - Sending and receiving work data using a VPN or work Wi-Fi network..... 21
    - Data flow: Sending email from a device using a VPN or work Wi-Fi network..... 21
    - Data flow: Receiving email on a device using a VPN or work Wi-Fi network..... 22
    - Data flow: Accessing an application or content server using a VPN or work Wi-Fi network..... 22
  
- Legal notice..... 24**

# BlackBerry UEM Cloud architecture and data flows

BlackBerry UEM Cloud is a unified endpoint management solution from BlackBerry. With BlackBerry UEM Cloud you can manage iOS, macOS, Android, and Windows 10 devices using a simple web-based interface and protect business information on BYOD, COPE, and COBO devices.

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

## Architecture: BlackBerry UEM Cloud solution



Component	Description
BlackBerry UEM Cloud	BlackBerry UEM Cloud is a service that allows you to manage devices used in your organization's environment.
BlackBerry Infrastructure and BlackBerry Dynamics NOC	<p>The BlackBerry Infrastructure registers user information for device activation and validates licensing information for BlackBerry UEM Cloud. If you enable BlackBerry Secure Connect Plus or the BlackBerry Secure Gateway, data in transit that uses these services passes through the BlackBerry Infrastructure.</p> <p>The BlackBerry Dynamics NOC is a separately located NOC that provides secure communications between BlackBerry Dynamics apps on devices and BlackBerry Proxy installed behind the firewall as part of the BlackBerry Connectivity Node.</p>
Devices	BlackBerry UEM Cloud supports iOS, macOS, Android, and Windows 10 devices.

Component	Description
Notification services	<p>BlackBerry UEM Cloud 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:</p> <ul style="list-style-type: none"> <li>• APNs is a service that Apple provides to send notifications to iOS and macOS devices.</li> <li>• FCM is a service that Google provides to send notifications to Android devices.</li> <li>• WNS is a service that Microsoft provides to send notifications to Windows 10 devices.</li> </ul>
BlackBerry Connectivity Node	<p>The BlackBerry Connectivity Node is an optional component that you install inside your organization's firewall. It includes five components that add functionality to BlackBerry UEM Cloud:</p> <ul style="list-style-type: none"> <li>• The BlackBerry Cloud Connector connects BlackBerry UEM Cloud to your company directory behind the firewall to allow basic attribute synchronization, search functionality, and user authentication services. If you don't install the BlackBerry Connectivity Node and your company directory is behind the firewall, you must create local user accounts in BlackBerry UEM Cloud instead of using the user accounts in your company directory. The BlackBerry Cloud Connector is not required for BlackBerry UEM Cloud to connect to Microsoft Azure Active Directory.</li> <li>• BlackBerry Proxy maintains a secure connection between your organization and the BlackBerry Dynamics NOC, which allows BlackBerry Dynamics apps to communicate securely with your organization's resources behind the firewall. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC.</li> <li>• The BlackBerry Gatekeeping Service sends commands to Exchange ActiveSync to add devices to an allowed list when devices are activated on BlackBerry UEM Cloud. Unmanaged devices that try to connect to an organization's mail server can be reviewed, verified, and blocked or allowed by an administrator using the BlackBerry UEM management console.</li> <li>• 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.</li> <li>• The BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and BlackBerry UEM Cloud to your organization's mail server for iOS devices.</li> </ul> <p>The BlackBerry Connectivity Node uses port 3101 to communicate with BlackBerry UEM Cloud.</p>

Component	Description
BlackBerry Enterprise Mobility Server	<p>If you have installed the BlackBerry Connectivity Node, you can also install an on-premises BEMS. BEMS consolidates several services used to send work data to and from BlackBerry Dynamics apps:</p> <ul style="list-style-type: none"> <li>• BlackBerry Connect provides secure instant messaging, company directory look-up, and user presence information to iOS and Android devices.</li> <li>• BlackBerry Presence provides real-time presence status to BlackBerry Dynamics apps.</li> <li>• 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.</li> </ul>
BlackBerry Enterprise Mobility Server databases	The BEMS databases store user, app, policy, and configuration information.
Company directory	BlackBerry UEM Cloud supports connectivity with your organization's Microsoft Active Directory or LDAP company directory behind the firewall using the BlackBerry Connectivity Node.
Microsoft Azure Active Directory	Microsoft Azure Active Directory is a cloud-based directory management service. If your organization uses Azure Active Directory you can connect to it instead of, or in addition to, a company directory behind the firewall.
Content, application, and mail servers	<p>When you enable BlackBerry Secure Connect Plus or when users have BlackBerry Dynamics apps, devices can connect to your organization's servers without requiring you to open a direct connection between the server and the Internet. Work data in transit between your servers and devices is sent through BlackBerry Secure Connect Plus and the BlackBerry Infrastructure. BlackBerry Dynamics app data is sent through BlackBerry Proxy and the BlackBerry Dynamics NOC.</p> <p>The BlackBerry Secure Gateway provides a secure connection through the BlackBerry Infrastructure and BlackBerry Connectivity Node between your organization's mail server and iOS devices.</p>
BlackBerry plug-ins and BEMS	<p>The cloud version of BlackBerry Enterprise Mobility Server provides BlackBerry Push Notifications, which 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. When you specify the on-premises Microsoft Exchange Server or Microsoft Office 365 server information, you specify the settings to create the BEMS Cloud tenant for your organization.</p> <p>You can also integrate the cloud version of BEMS with BlackBerry Docs, which 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.</p> <p>BlackBerry UEM Cloud works with additional BlackBerry enterprise products such as BlackBerry Enterprise Identity, BlackBerry 2FA, and BlackBerry Workspaces, to allow you to extend UEM capabilities in your organization.</p>

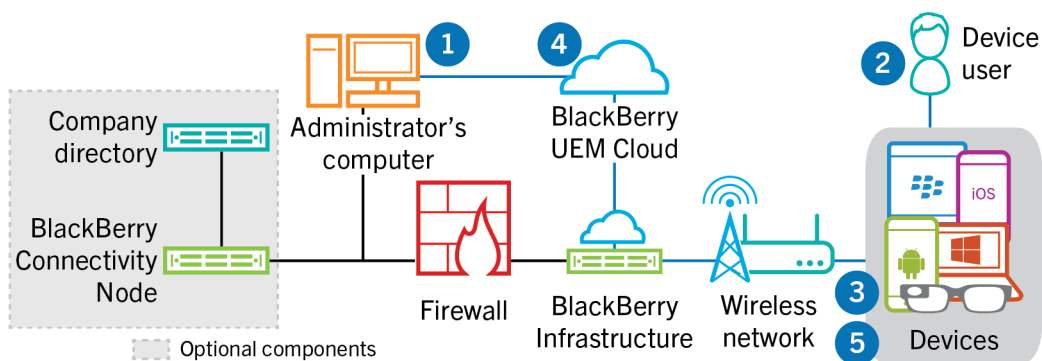
# Activating devices and BlackBerry Dynamics apps

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 iOS, Android, or Windows 10 device

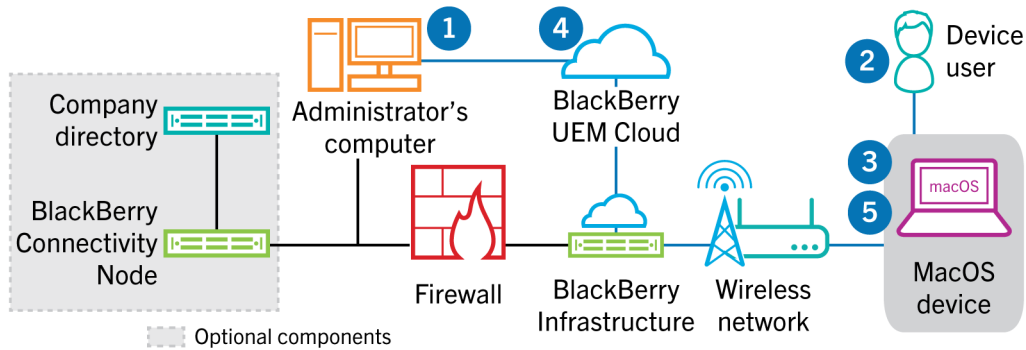


1. You perform the following actions:
  - a. Add a user to BlackBerry UEM Cloud as a local user account or, if you installed the BlackBerry Connectivity Node, using the account information retrieved from your company directory.
  - b. Assign an activation profile to the user.
  - c. Depending on the device type and your organization's preferences, 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 message 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 or view a QR code.
2. The user performs the following actions:
  - a. If activating an iOS or Android device, downloads and installs the BlackBerry UEM Client.
  - b. Enters their activation username and password or scans the QR code on their device.
3. The device sends an activation request to BlackBerry UEM.

4. BlackBerry UEM Cloud verifies the user's activation credentials and sends the activation details to the device, including device configuration information.
5. The device receives the activation details from BlackBerry UEM Cloud and completes the configuration. The device then sends confirmation to BlackBerry UEM Cloud that the activation was successful.



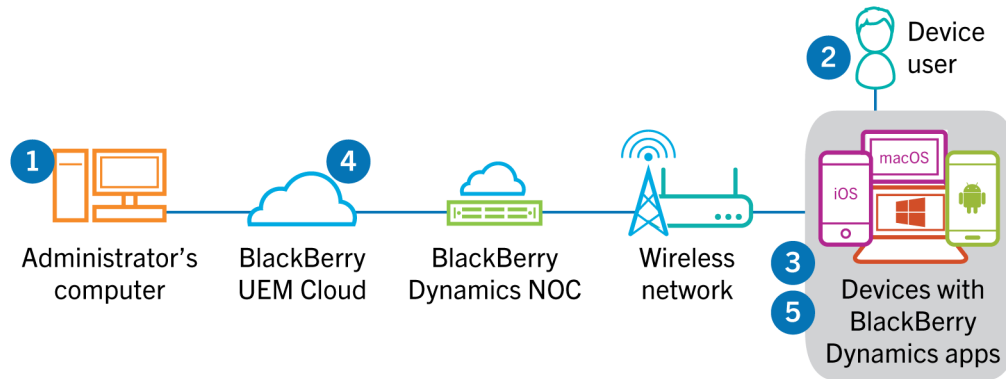
## Data flow: Activating a macOS device



1. You perform the following actions:
  - a. Add the user to BlackBerry UEM Cloud as a local user account or, if you installed the BlackBerry Connectivity Node, using the account information retrieved from your company directory.
  - b. Assign an activation profile to the user.
  - c. Make sure that the user has 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 Cloud.
4. BlackBerry UEM Cloud verifies the activation credentials and sends the activation details to the device, including device configuration information.
5. The device receives the activation details from BlackBerry UEM Cloud and completes the configuration. The device then sends confirmation to BlackBerry UEM Cloud that the activation was successful.

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

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

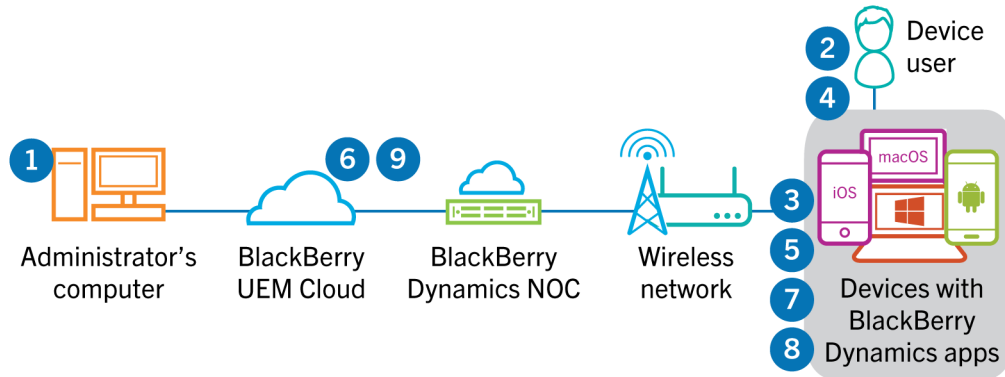


1. An administrator performs the following actions:
  - a. Assigns one or more BlackBerry Dynamics apps to a user.
  - b. Issues activation credentials (access key, activation password, or QR code) or using a third-party identity provider, and sends them to the user or instructs the user to generate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

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

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

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



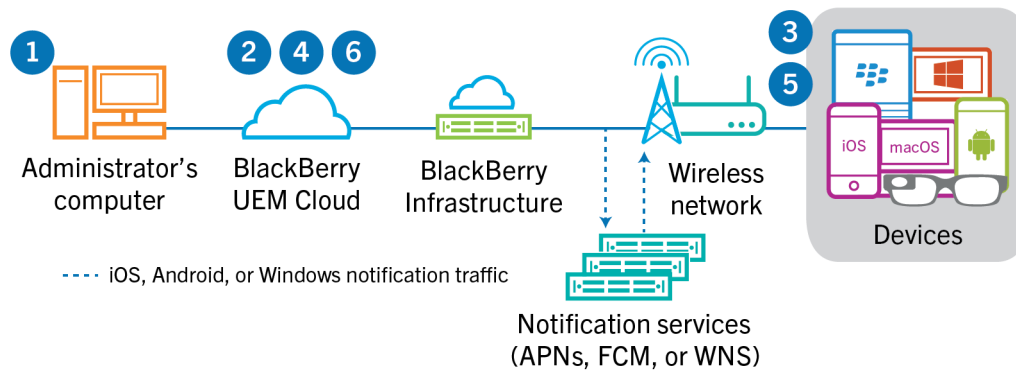
1. An administrator assigns one or more BlackBerry Dynamics apps to a user.
2. The user installs the app on the device.
3. The app performs the following actions:
  - a. Queries the BlackBerry Dynamics NOC and identifies another app that is activated on the device
  - b. Requests the activation credentials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

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

# Data flow: Receiving configuration updates on a device

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 IT 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 Cloud notifies the device that a configuration update is pending. Devices also poll BlackBerry UEM Cloud 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.



1. You use the management console to send device commands, such as lock device or delete the work data, or you perform device management tasks, such as updates to IT policy, profile, or app settings or assignments, and trigger a configuration update for the device.
2. BlackBerry UEM Cloud assigns the update and identifies the objects that must be shared with the device then performs one of the following actions:
  - For Android devices, BlackBerry UEM Cloud notifies the BlackBerry UEM Client on the device that an update is pending using the FCM. The FCM sends a notification to the device to contact BlackBerry UEM Cloud.
  - For iOS and OS X devices, BlackBerry UEM Cloud notifies the MDM Daemon on the device that an update is pending using the APNs. The APNs sends a notification to the device to contact BlackBerry UEM Cloud.
  - For Windows 10 devices, BlackBerry UEM Cloud notifies the MDM Daemon on the device that an update is pending using the WNS. The WNS sends a notification to the device to contact BlackBerry UEM Cloud.
3. The device contacts BlackBerry UEM Cloud to request any pending actions that must be performed on the device.
4. BlackBerry UEM Cloud replies with the highest priority action.

Priority is given to IT administration commands, such as Lock device, followed by requests for device information, installed apps, and so on. BlackBerry UEM Cloud sends one command at a time. If necessary, additional information is included in the response.
5. The device performs the following actions:
  - a. Inspects the response from BlackBerry UEM Cloud
  - b. Schedules the command to be processed, and waits for the command to run
  - c. Sends a response to BlackBerry UEM Cloud to update the command status. The status indicates whether the command ran successfully and provides an error message in the event of a failure.
6. If more actions or commands are pending for the device, BlackBerry UEM Cloud replies with the highest priority action.

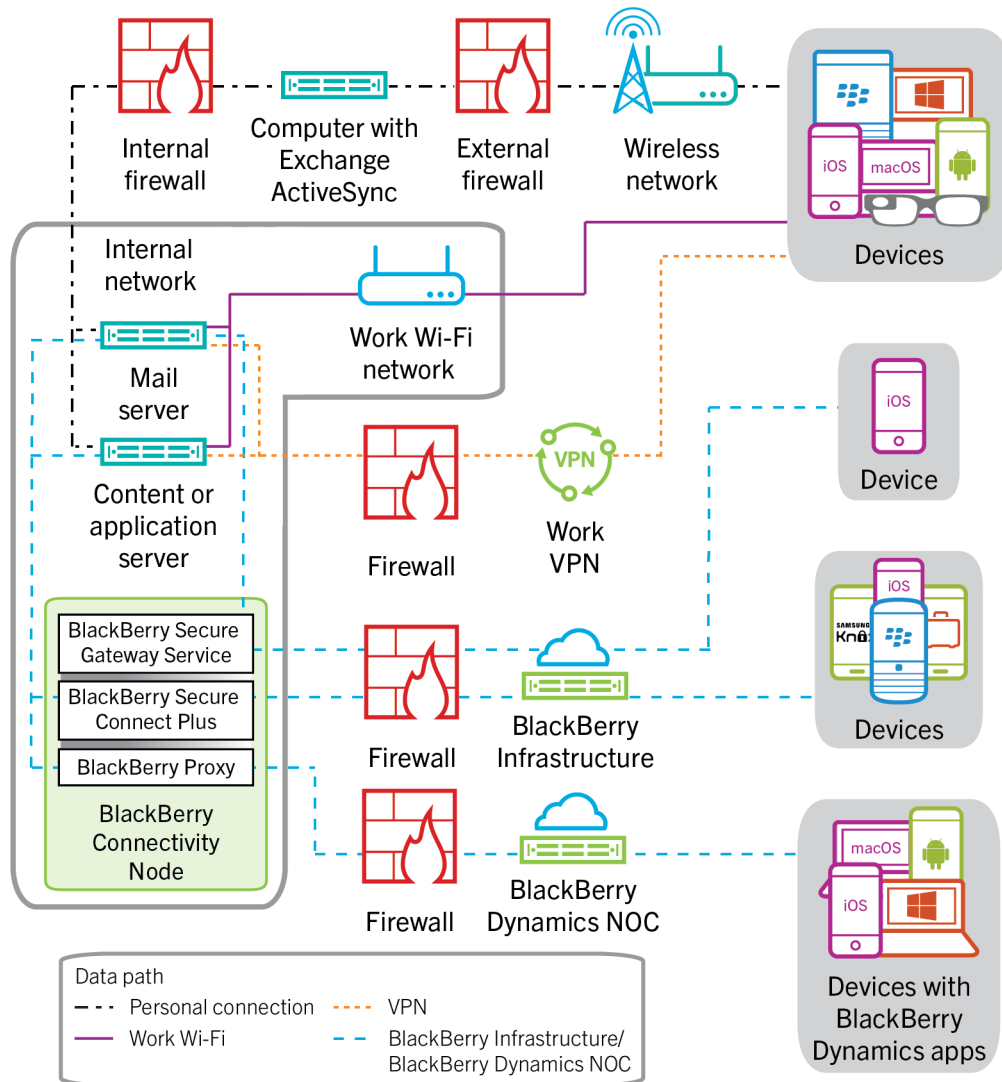
Steps 4 to 6 repeat until no more pending actions or commands must be performed and BlackBerry UEM Cloud replies with an idle command.

# Sending and receiving work data

When users send and receive work data on a device, data can travel between the device and your resources using the following connections:

- The device can use a direct connection over the or mobile network from the device to the mail, content, or application server (for example, an Exchange ActiveSync server that is placed in a DMZ or is exposed to the public network).
- The device can use a direct connection through your organization's VPN or work Wi-Fi network to the mail, content, or application server. The device VPN or Wi-Fi profile may be configured by you or by the users.
- If you install the BlackBerry Connectivity Node, BlackBerry Secure Connect Plus can provide a secure IP tunnel through the BlackBerry Infrastructure between apps on iOS, Android Enterprise , and Samsung Knox Workspace devices and your organization's network.
- If you install the BlackBerry Connectivity Node, BlackBerry Proxy can provide a secure connection between BlackBerry Dynamics apps on devices and your organization's network.
- If you install the BlackBerry Connectivity Node, the BlackBerry Secure Gateway can provide a secure connection through the BlackBerry Infrastructure and BlackBerry UEM to your organization's mail server for iOS devices.

This diagram shows the possible data paths.

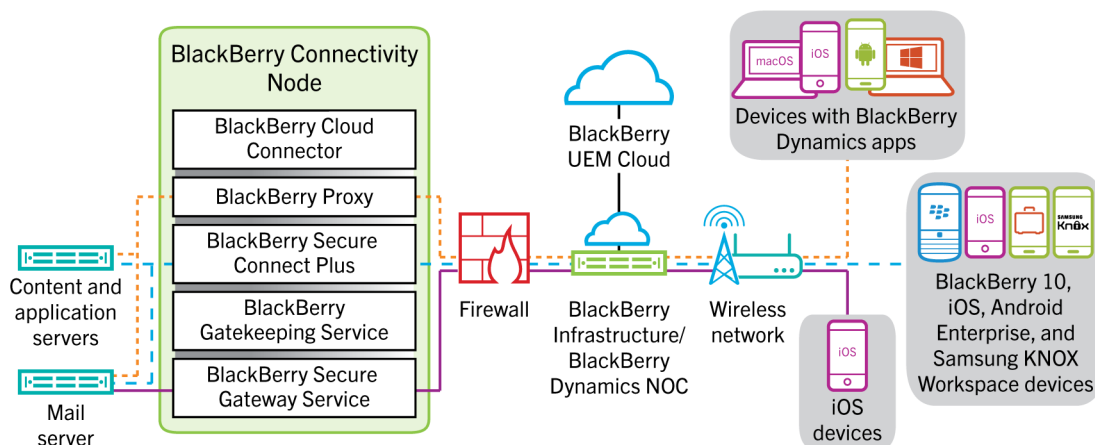


# Sending and receiving work data using BlackBerry UEM Cloud and the BlackBerry Infrastructure

If you install the BlackBerry Connectivity Node, devices can connect to your organization's resources through BlackBerry UEM Cloud and the BlackBerry Infrastructure or the BlackBerry Dynamics NOC using the following services:

Service	Description
BlackBerry Secure Connect Plus	<p>BlackBerry Secure Connect Plus provides a secure IP tunnel through the BlackBerry Infrastructure to transfer data between apps and your organization's network.</p> <p>For Android Enterprise devices, BlackBerry Secure Connect Plus provides a secure tunnel between all work space apps and your organization's network.</p> <p>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.</p> <p>For iOS devices, BlackBerry Secure Connect Plus can provide a secure tunnel between your organization's network and all apps or only specified apps.</p>
BlackBerry Proxy	BlackBerry Proxy provides a secure connection between BlackBerry Dynamics apps on devices and your organization's resources behind the firewall. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC.
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.

The following diagram shows how devices can connect to your organization's resources through the BlackBerry Infrastructure and BlackBerry UEM Cloud.

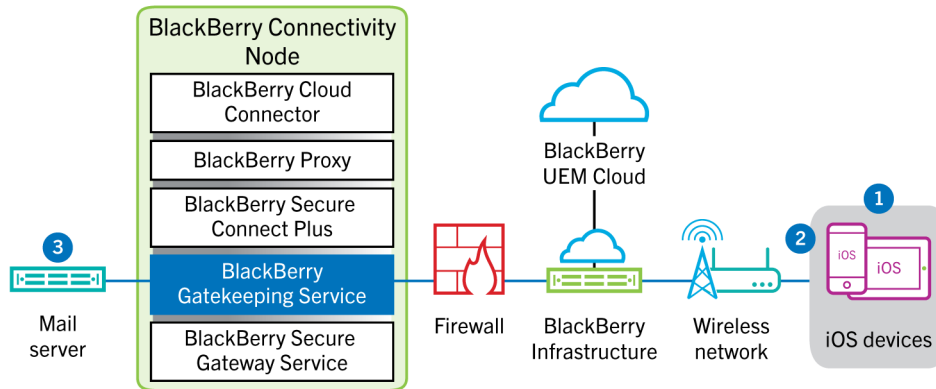


For more information about enabling BlackBerry Secure Connect Plus, see ["Enabling and configuring BlackBerry Secure Connect Plus" in the Administration content.](#)

For more information about enabling the BlackBerry Secure Gateway, see ["Protecting email data using the BlackBerry Secure Gateway"](#) in the Administration content.

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

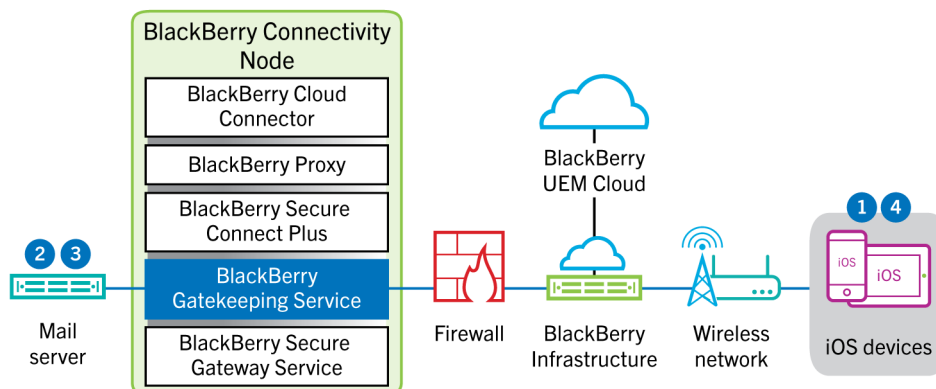
This data flow describes how work email and calendar data travels from iOS devices to the Exchange ActiveSync server using the BlackBerry Secure Gateway.



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.



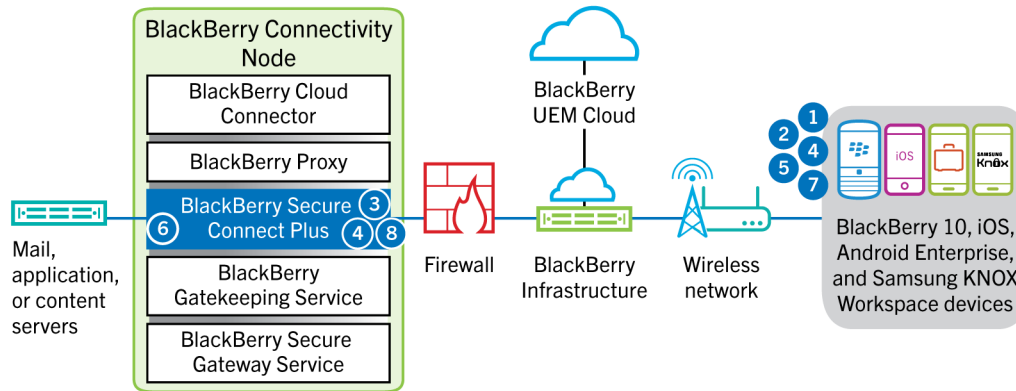
1. The device issues an HTTPS request to the mail server and requests that the mail server notify the device when any items change in the folders that are configured for synchronization. The request travels through the encrypted and authenticated channel between the BlackBerry Infrastructure and the BlackBerry Secure Gateway to the mail server.
2. If there are no new or changed items during this interval, the mail server sends an "HTTP 200 OK" message to the device. The device issues a new request and the process starts over.
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 through the secure channel between the BlackBerry Secure Gateway and the BlackBerry Infrastructure to the email or organizer app on the device.



- When the synchronization is complete, the device issues another request to restart the process.

### Data flow: Sending and receiving work data 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.



- The user opens an app to access work data from a content or application server behind your organization's firewall.
  - On Android Enterprise, and Samsung Knox Workspace devices, all work apps can use BlackBerry Secure Connect Plus.
  - On iOS devices, you specify whether all apps or only specified apps can use BlackBerry Secure Connect Plus.
- The device determines that a secure IP tunnel is the most direct, cost-efficient method available to connect to the application or content server to retrieve the data and sends a request through a TLS tunnel, over port 443, to the BlackBerry Infrastructure for a secure tunnel to the work network. By default, the signal is encrypted using FIPS-140 certified Certicom libraries. The signaling tunnel is encrypted end-to-end.
- BlackBerry Secure Connect Plus receives the request from the BlackBerry Infrastructure through port 3101.
- 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.
- The app uses the tunnel to connect to the application or content server using standard IPv4 protocols (TCP and UDP).
- 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.
- The app receives and displays the data on the device.
- 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.

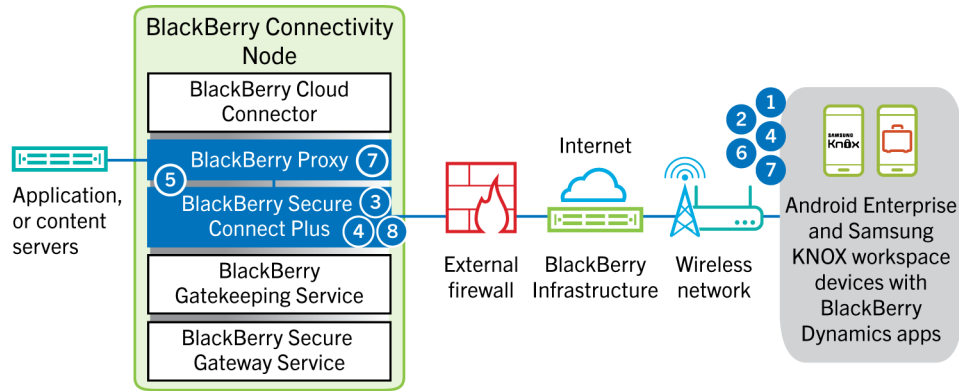
For iOS devices, if you configure per-app VPN for BlackBerry Secure Connect Plus, the tunnel eventually terminates when none of the configured apps are in use.

### 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.

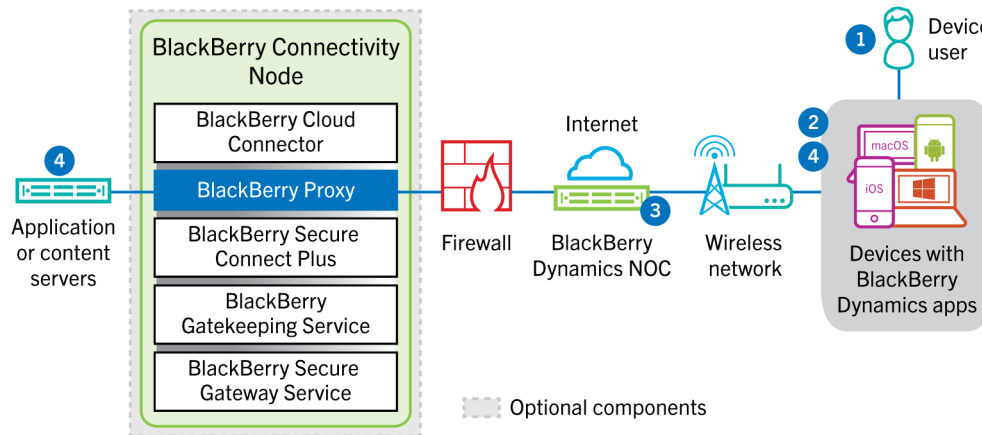
If you are using BlackBerry Secure Connect Plus with BlackBerry Dynamics apps on an Android Enterprise device or a Samsung Knox Workspace device, it is recommended that you configure BlackBerry UEM not to send BlackBerry Dynamics app data through the BlackBerry Dynamics NOC to reduce network latency.



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 and receiving work data from a BlackBerry Dynamics app

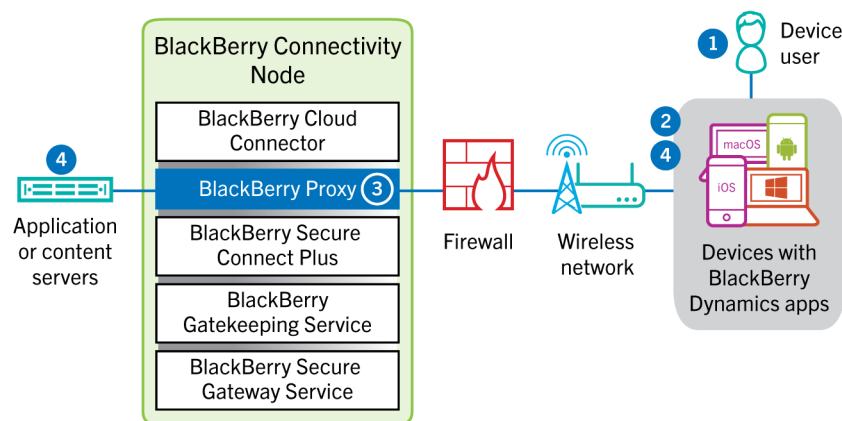
This data flow describes how data travels when a BlackBerry Dynamics app accesses an application or content server in your organization.



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 performs one of the following actions:
  - a. Communicates with BlackBerry Proxy over a pre-established secure connection to establish an end-to-end connection over port 443 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.
  - b. If the BlackBerry Connectivity Node is not configured, communicates directly with your application or content servers through a port you have opened in your organization's firewall.
4. If the BlackBerry Connectivity Node is configured, once the secure end-to-end connection is established between the BlackBerry Dynamics NOC and BlackBerry Proxy, 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 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 Proxy.



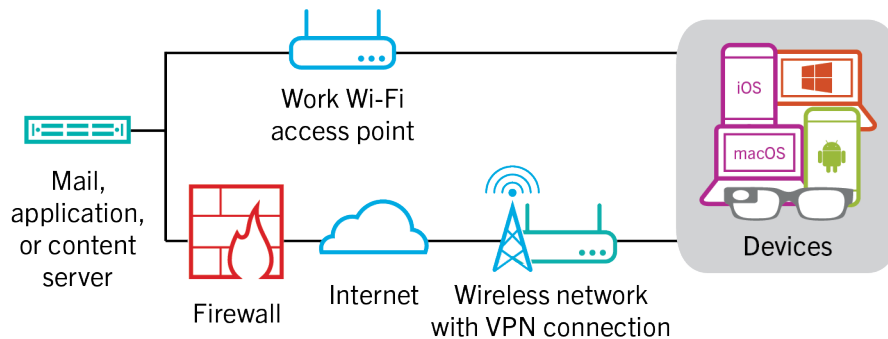
1. The user opens a BlackBerry Dynamics app to access work data.
2. The BlackBerry Dynamics app establishes a TLS connection to BlackBerry Proxy over port 17533.
3. BlackBerry Proxy authenticates with the BlackBerry Dynamics app. BlackBerry Proxy authenticates with the app using its server certificate. 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.

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

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

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

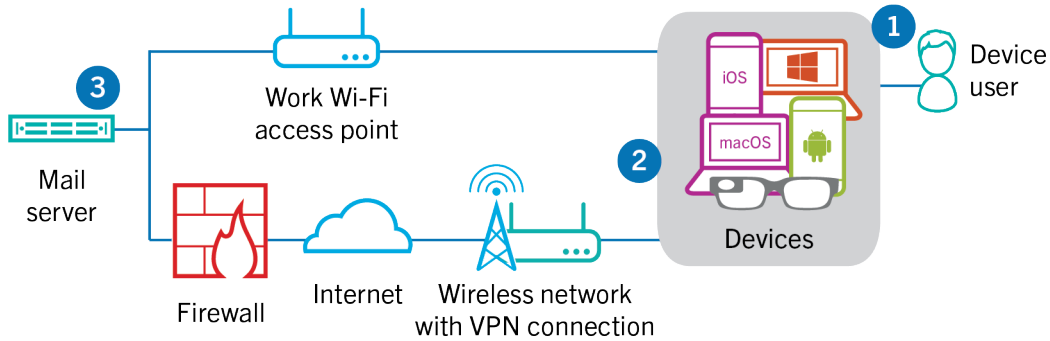


The following table describes when devices use your organization's VPN or work Wi-Fi network to connect to your organization's network.

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

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

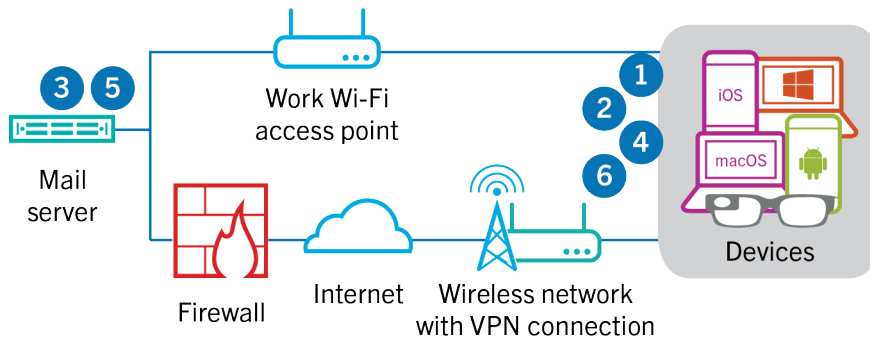
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



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

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

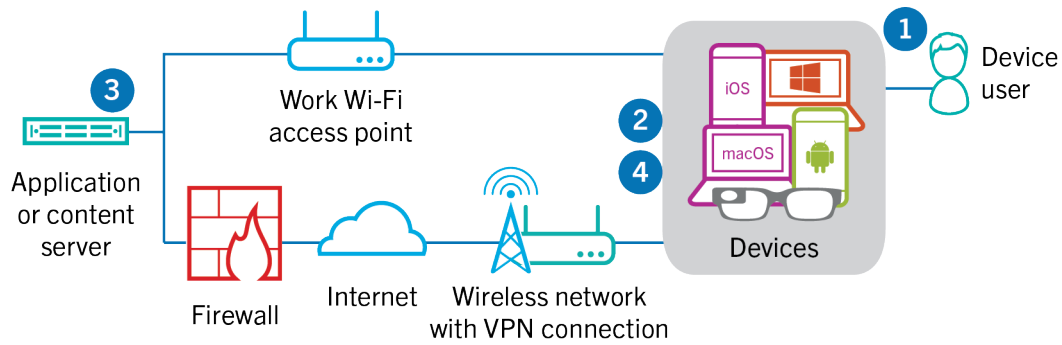
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



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

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

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



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

# Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

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

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

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



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

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

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

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

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

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

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

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

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

Published in Canada