

# Reference Guide

What's New in BES12 Cloud  
711-60712-123





# Contents

What's new in BES12 Cloud .....	5
Supported features by device type.....	5
Compatibility and requirements.....	11
BES12 Cloud Architecture and data flows.....	12
Architecture: BES12 Cloud solution.....	12
Architecture: BES12 Cloud and BlackBerry Secure Connect Plus.....	14
Architecture: BES12 Cloud and the BlackBerry Gatekeeping Service.....	15
Architecture: Android for Work.....	16
Architecture: KNOX Workspace.....	17
Activating devices.....	19
Data flow: Activating a BlackBerry 10, iOS, Android, or Windows device.....	19
Data flow: Activating an OS X device.....	21
Data flow: Receiving configuration updates on a device.....	22
Sending and receiving work data.....	24
Using your organization's VPN or work Wi-Fi network.....	25
Using BES12 Cloud and the BlackBerry Infrastructure.....	28
Administrators.....	30
Send an email to users.....	30
Set an expiry time for commands.....	30
Windows 10 apps.....	32
Add a Windows 10 app to the app list.....	32
Configuring BES12 to synchronize with the Windows Store for Business.....	32
BlackBerry Secure Connect Plus.....	36
Using BlackBerry Secure Connect Plus for secure connections to work resources.....	36
Steps to enable BlackBerry Secure Connect Plus.....	37
Server and device requirements.....	37
Installing or upgrading the BlackBerry Secure Connect Plus component.....	38
Enabling and configuring BlackBerry Secure Connect Plus.....	39
Integrating BES12 with your organization's PKI software.....	43
Connect BES12 to your organization's OpenTrust software.....	43
Using Exchange Gatekeeping.....	45
Controlling which devices can access Exchange ActiveSync.....	45
Configure Microsoft IIS permissions for gatekeeping.....	48
Create a gatekeeping configuration.....	49

Allow a device to access Microsoft ActiveSync.....	50
Block a device from accessing Microsoft ActiveSync.....	50
Product documentation.....	51
Glossary.....	53
Legal notice.....	55

# What's new in BES12 Cloud

## Supported features by device type

This quick reference compares the supported capabilities of BlackBerry 10, iOS, OS X, Android, and Windows devices in BES12 version 12.4.

For more information about supported OS versions, [see the Compatibility matrix](#).

### Device features

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
Wireless activation	√	√	√	√	√	√
Wired activation using the BlackBerry Wired Activation Tool	√					
Client app required for activation			√ <sup>1</sup>		√	√ <sup>2</sup>
Customize terms of use agreement for activation	√		√	√		√ <sup>3</sup>
Restrict activation by device model	√		√	√	√	√ <sup>4</sup>
View and export device report (for example, hardware details)	√	√	√	√	√	√

<sup>1</sup> For iOS devices enrolled in DEP, client app must be assigned to users or groups.

<sup>2</sup> For Windows Phone 8.x devices only.

<sup>3</sup> For Windows 10 devices only.

<sup>4</sup> For Windows Phone 8.x and Windows 10 Mobile devices only.

## Security features

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
Separation of work and personal data	√	√	√ <sup>1</sup>		√ <sup>2</sup>	
User privacy for personal data	√	√	√ <sup>1</sup>		√ <sup>2</sup>	
Encryption of work data at rest	√	√	√ <sup>1</sup>		√ <sup>2</sup>	
Protection of devices by sending IT commands	√	√	√	√	√	√
Control of device capabilities using IT policies	√	√	√	√	√	√
Delete work data after period of inactivity	√		√ <sup>1</sup>		√ <sup>1</sup>	
Enforce password requirements	√	√	√	√	√	√
Enforce encryption of media card	√	√			√ <sup>3</sup>	
Enforce encryption of internal storage	√	√			√	√

<sup>1</sup> Requires Secure Work Space or Good Dynamics apps.

<sup>2</sup> Requires Secure Work Space, Samsung KNOX Workspace, Android for Work, or Good Dynamics apps.

<sup>3</sup> For Samsung KNOX devices only.

## Sending certificates to devices

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
CA certificate profiles	√		√	√	√	√
SCEP profiles	√		√	√	√	√ <sup>1</sup>
Shared certificate profiles			√	√	√	
User credential profiles	√		√	√	√	

<sup>1</sup> For Windows 10 devices only.

## Managing work connections for devices

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
CalDAV profiles			√	√		
CardDAV profiles			√	√		
Certificate retrieval profiles	√		√ <sup>1</sup>		√ <sup>1</sup>	
Enterprise connectivity	√		√ <sup>1</sup>		√ <sup>1</sup>	
BlackBerry Secure Connect Plus	√		√ <sup>2</sup>		√ <sup>3</sup>	
Exchange ActiveSync email profiles	√		√	√	√ <sup>4</sup>	√
IMAP/POP3 email profiles			√	√	√	√
Proxy profiles	√		√	√	√	√ <sup>5</sup>
Single sign-on profiles	√		√			

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
VPN profiles	√	√	√	√	√ <sup>6</sup>	√ <sup>7</sup>
Wi-Fi profiles	√	√	√	√	√	√
Other OS-specific profiles	<ul style="list-style-type: none"> <li>• CRL profiles</li> <li>• OCSP profiles</li> </ul>					

<sup>1</sup> Only for devices with Secure Work Space.

<sup>2</sup> Only for devices running iOS 9.0 and later.

<sup>3</sup> Only for Android for Work and KNOX Workspace devices.

<sup>4</sup> Only for devices with the TouchDown app installed, Motorola devices that support the EDM API, Android for Work devices, and KNOX devices.

<sup>5</sup> Only for Windows 10 devices (configure proxy settings in VPN profiles) and Windows 10 Mobile devices (configure proxy settings in Wi-Fi profiles).

<sup>6</sup> For KNOX Workspace devices only.

<sup>7</sup> For Windows 10 devices only.

## Managing your organization's standards for devices

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
Activation profiles	√		√	√	√	√
App lock mode profiles			√ <sup>1</sup>		√ <sup>1</sup>	
Compliance profiles	√		√		√	√ <sup>2</sup>
Device profiles	√		√		√	√ <sup>3</sup>
Enterprise Management Agent profiles	√		√		√	√
Good Dynamics profiles			√		√	
Location service profiles			√		√	√ <sup>4</sup>



Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
Web icon profiles			√	√		
Other OS-specific profiles	<ul style="list-style-type: none"> <li>• Device SR requirements profiles</li> </ul>	<ul style="list-style-type: none"> <li>• Access control rules</li> <li>• Software configuration</li> </ul>	<ul style="list-style-type: none"> <li>• AirPlay profiles</li> <li>• AirPrint profiles</li> <li>• Custom payload profiles</li> <li>• Managed domains profiles</li> <li>• Network usage profiles</li> <li>• Web content filter profiles</li> </ul>			

<sup>1</sup> Only for supervised iOS devices and KNOX devices that are activated with MDM controls.

<sup>2</sup> For Windows Phone 8.x devices only.

<sup>3</sup> For Windows 10 devices only.

<sup>4</sup> For Windows 10 Mobile devices only.

## Protecting lost or stolen devices

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
Specify device password	√	√			√	√ <sup>1</sup>
Lock device	√	√	√	√	√	√ <sup>1</sup>
Unlock device and clear password			√		√	
Delete all device data	√	√	√	√	√ <sup>2</sup>	√
Delete only work data	√	√	√	√	√	√

<sup>1</sup> For Windows Phone 8.x and Windows 10 Mobile devices only.

<sup>2</sup> For Motorola devices that support the EDM API, information on the media card is also deleted. For KNOX Workspace devices, you can choose to delete information on the media card.

## Configuring roaming

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
Disable automatic synchronization when roaming	√ <sup>1</sup>		√		√ <sup>2</sup>	
Disable data when roaming	√				√ <sup>2</sup>	√

<sup>1</sup> For synchronization with the mail server only.

<sup>2</sup> For KNOX devices only.

## Managing apps

Feature	BlackBerry 10	BlackBerry OS	iOS	OS X	Android	Windows
Distribute public apps from storefront (BlackBerry World, App Store, Google Play, Windows Store)	√		√		√	√
Manage work app catalog	√	√	√		√	√
Brand work app catalog	√		√			
Manage restricted apps			√		√ <sup>1</sup>	√ <sup>1</sup>
Distribute internal apps	√	√	√		√	√

<sup>1</sup> The restricted app list is not required for Android for Work, KNOX Workspace, or Windows 10 devices because only apps that an administrator assigns can be installed in the work space or on devices.

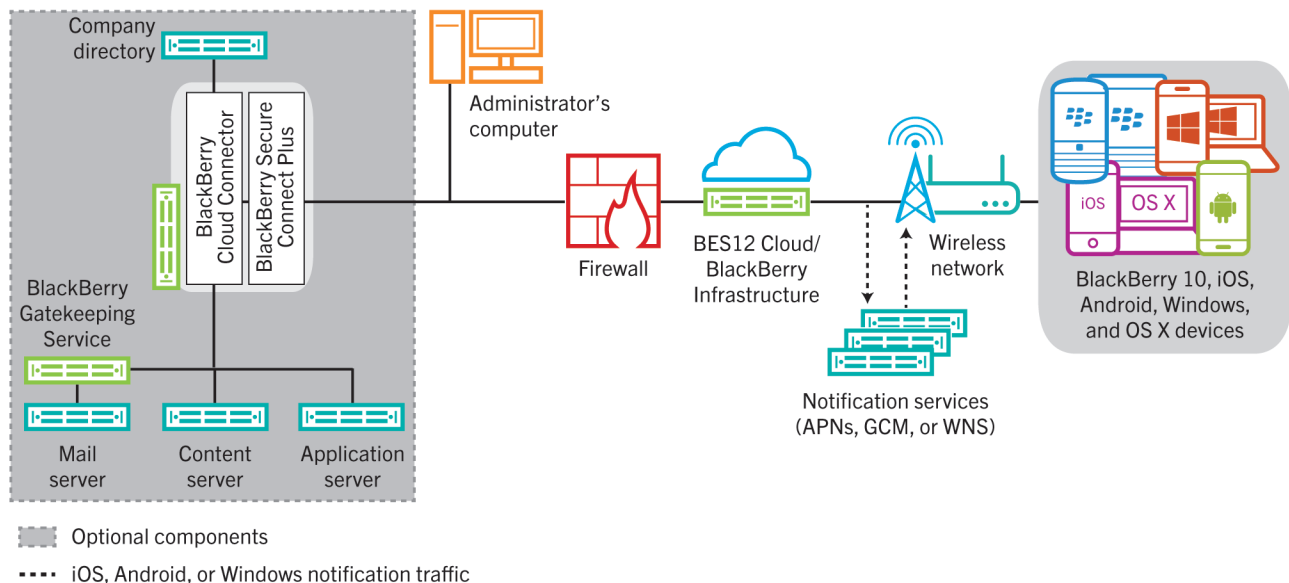
## Compatibility and requirements

You can find up-to-date information about compatibility, including device types, operating systems for devices, and browsers for accessing BES12 Cloud, [in the BES12 Cloud Compatibility matrix..](#)

# BES12 Cloud Architecture and data flows

The BES12 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.

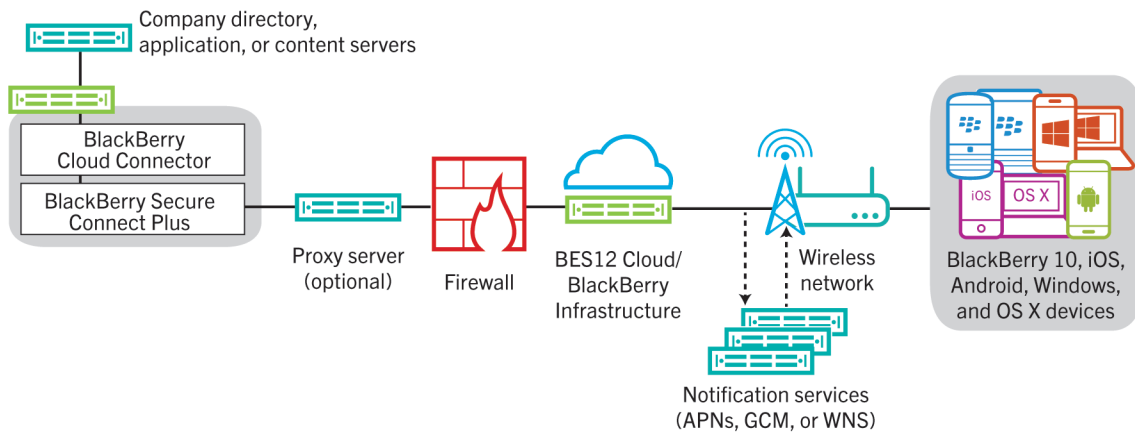
## Architecture: BES12 Cloud solution



Component	Description
BES12 Cloud	BES12 Cloud is a service that allows you to manage devices used in your organization's environment.
BlackBerry Cloud Connector	The BlackBerry Cloud Connector is an optional component that you install inside your organization's firewall. It connects your company directory to BES12 Cloud

Component	Description
	<p>to allow basic attribute synchronization, search functionality, and user authentication services.</p> <p>The BlackBerry Cloud Connector uses port 3101 to communicate with BES12 Cloud.</p> <p>If you do not use the BlackBerry Cloud Connector you must create local user accounts in BES12 Cloud instead of using the user accounts in your company directory.</p> <p>When you install or upgrade the BlackBerry Cloud Connector, the setup process also installs the BlackBerry Secure Connect Plus component on the same computer.</p>
BlackBerry Secure Connect Plus	<p>BlackBerry Secure Connect Plus is an optional component that is installed with the BlackBerry Cloud Connector inside your organization's firewall. BlackBerry Secure Connect Plus establishes a secure IP tunnel between apps on devices and your organization's network through the BlackBerry Infrastructure:</p> <ul style="list-style-type: none"> <li>• On BlackBerry 10, Samsung KNOX Workspace, and Android for Work devices, all work space apps use the secure tunnel.</li> </ul> <p>This tunnel gives users access to work resources behind your organization's firewall while ensuring the security of data using standard protocols and end-to-end encryption.</p>
BlackBerry Infrastructure	<p>The BlackBerry Infrastructure registers user information for device activation and validates licensing information for BES12 Cloud.</p>
Devices	<p>BES12 Cloud supports BlackBerry 10, iOS, Android, Windows, and OS X devices.</p>
Notification services	<p>BES12 Cloud sends notifications to devices to contact BES12 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 OS X devices.</li> <li>• GCM 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 devices.</li> </ul>
Company directory	<p>BES12 Cloud supports connectivity with your organization's Microsoft Active Directory or LDAP company directory using the BlackBerry Cloud Connector.</p>
Content, application, and mail servers	<p>When you enable BlackBerry Secure Connect Plus, devices can connect to your organization's servers without requiring you to open a direct connection to the Internet. Work data in transit between your servers and devices is sent through BlackBerry Secure Connect Plus and the BlackBerry Infrastructure.</p>

# Architecture: BES12 Cloud and BlackBerry Secure Connect Plus

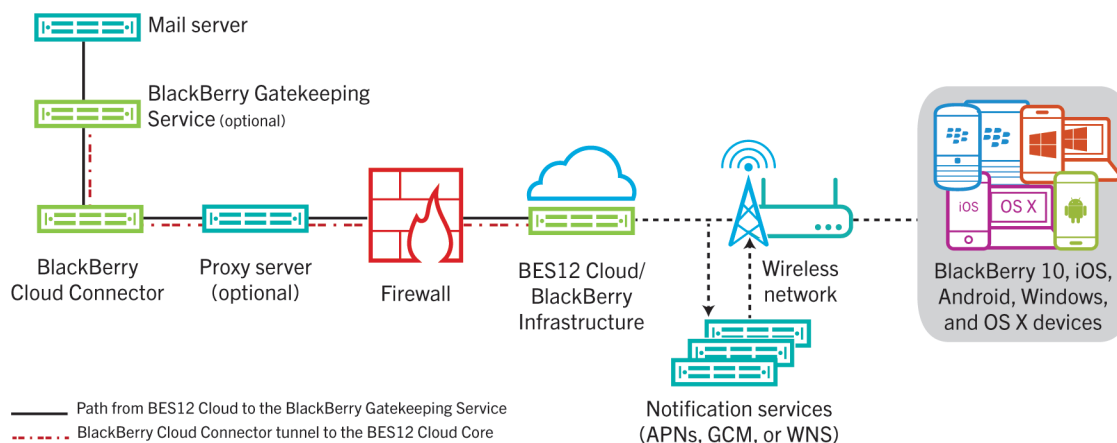


The diagram above shows the components that the BlackBerry Cloud Connector interacts with. For more information about the BES12 Cloud architecture, [see the Overview and what's new content](#).

Component	Description
BlackBerry Cloud Connector	The BlackBerry Cloud Connector is a Java process that provides a secure connection through your firewall for communication between BES12 Cloud and your company directory. You install the BlackBerry Cloud Connector behind your organization's firewall. Using the management console, you activate the BlackBerry Cloud Connector with BES12 Cloud and you connect it to the company directory.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus is a BES12 component that provides a secure IP tunnel between apps and your organization's network: <ul style="list-style-type: none"> <li>For BlackBerry 10, Samsung KNOX Workspace, and Android for Work devices, all work space apps use the secure tunnel.</li> </ul> This tunnel gives users access to work resources behind your organization's firewall while ensuring the security of data using standard protocols and end-to-end encryption.
Company directory	The company directory is any service that your organization uses to manage user accounts for employees. BES12 Cloud supports: <ul style="list-style-type: none"> <li>Microsoft Active Directory</li> <li>LDAP</li> </ul>

Component	Description
Proxy server (optional)	You can configure the BlackBerry Cloud Connector to send data to and from BES12 Cloud through a proxy server that is behind your organization's firewall.
BES12 Cloud	BES12 Cloud is a cloud-based service hosted in the BlackBerry Infrastructure that you can use to manage BlackBerry 10, iOS, OS X, Android, and Windows Phone devices. You access the management console, which is hosted in the cloud, to manage users' devices.

## Architecture: BES12 Cloud and the BlackBerry Gatekeeping Service

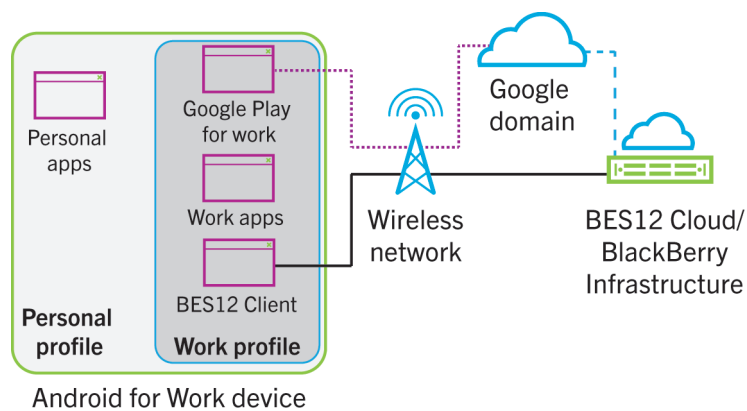


The diagram above shows the components that the BlackBerry Cloud Connector interacts with. For more information about the BES12 Cloud architecture, [see the Overview and what's new content](#).

Component	Description
BlackBerry Cloud Connector	The BlackBerry Cloud Connector is a Java process that provides a secure connection through your firewall for communication between BES12 Cloud and your company directory. You install the BlackBerry Cloud Connector behind your organization's firewall. Using the management console, you activate the BlackBerry Cloud Connector with BES12 Cloud and you connect it to the company directory.
BlackBerry Gatekeeping Service	The BlackBerry Gatekeeping Service is used to control which devices can access Exchange ActiveSync. Any device that is not whitelisted for Microsoft Exchange is reported in the BES12 Restricted Exchange ActiveSync devices list.

Component	Description
Company directory	The company directory is any service that your organization uses to manage user accounts for employees. BES12 Cloud supports: <ul style="list-style-type: none"> <li>• Microsoft Active Directory</li> <li>• LDAP</li> </ul>
Proxy server (optional)	You can configure the BlackBerry Cloud Connector to send data to and from BES12 Cloud through a proxy server that is behind your organization's firewall.
BES12 Cloud	BES12 Cloud is a cloud-based service hosted in the BlackBerry Infrastructure that you can use to manage BlackBerry 10, iOS, OS X, Android, and Windows Phone devices. You access the management console, which is hosted in the cloud, to manage users' devices.

## Architecture: Android for Work

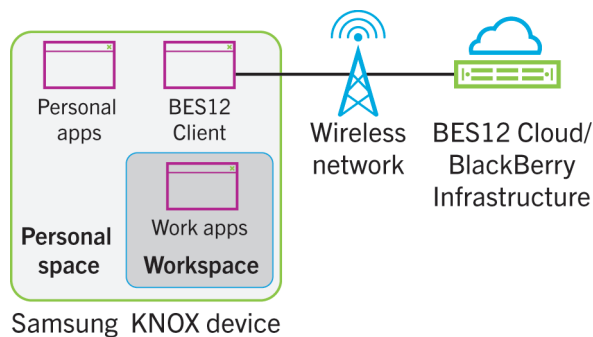


Component	Description
Android for Work device	Android for Work devices are Android devices that are activated on BES12 and use Android for Work.
Personal profile	The personal profile includes the personal apps and the Android platform and services (for example, the clipboard app).  If you activate the device using the Work and personal – user privacy (Android For Work) or Work and personal – user privacy (Android For Work – Premium) activation type, you can manage aspects of the personal profile using IT policy rules.
Work profile	The work profile is created when you activate the device on BES12 using an Android for Work activation type. It includes the following apps:



Component	Description
	<ul style="list-style-type: none"> <li>BES12 Client connects to BES12 to receive management commands.</li> <li>Google Play for Work connects to your organization's Google domain to download and install work apps.</li> <li>Work apps connect to your organization's network to access data. If an app can run in both the personal profile and the work profile (for example, Google Chrome), a separate instance of the app is copied into the work profile.</li> </ul>
Google domain	<p>The Google domain for your organization allows you to manage users and work apps. There are two types of Google domains:</p> <ul style="list-style-type: none"> <li>A managed Google domain which exists when your organization uses Google for email, calendar, and so on.</li> <li>A Google Apps domain which exists if your organization uses another mail solution (for example, Microsoft Exchange), and requires Google accounts only to manage Android for Work devices.</li> </ul>
BlackBerry Infrastructure	The BlackBerry Infrastructure registers user information for device activation. It also provides the connection to the Google domain so that BES12 can access your organization's Google directory and Google Play for Work.
BES12 Cloud	BES12 Cloud is the EMM solution by BlackBerry that you can use to manage Android for Work devices.

## Architecture: KNOX Workspace



Component	Description
Samsung KNOX device	A Samsung KNOX device is a Samsung device that supports KNOX Workspace and is activated using BES12.
Personal space	The personal space on a Samsung KNOX device includes the personal apps and the Android OS.

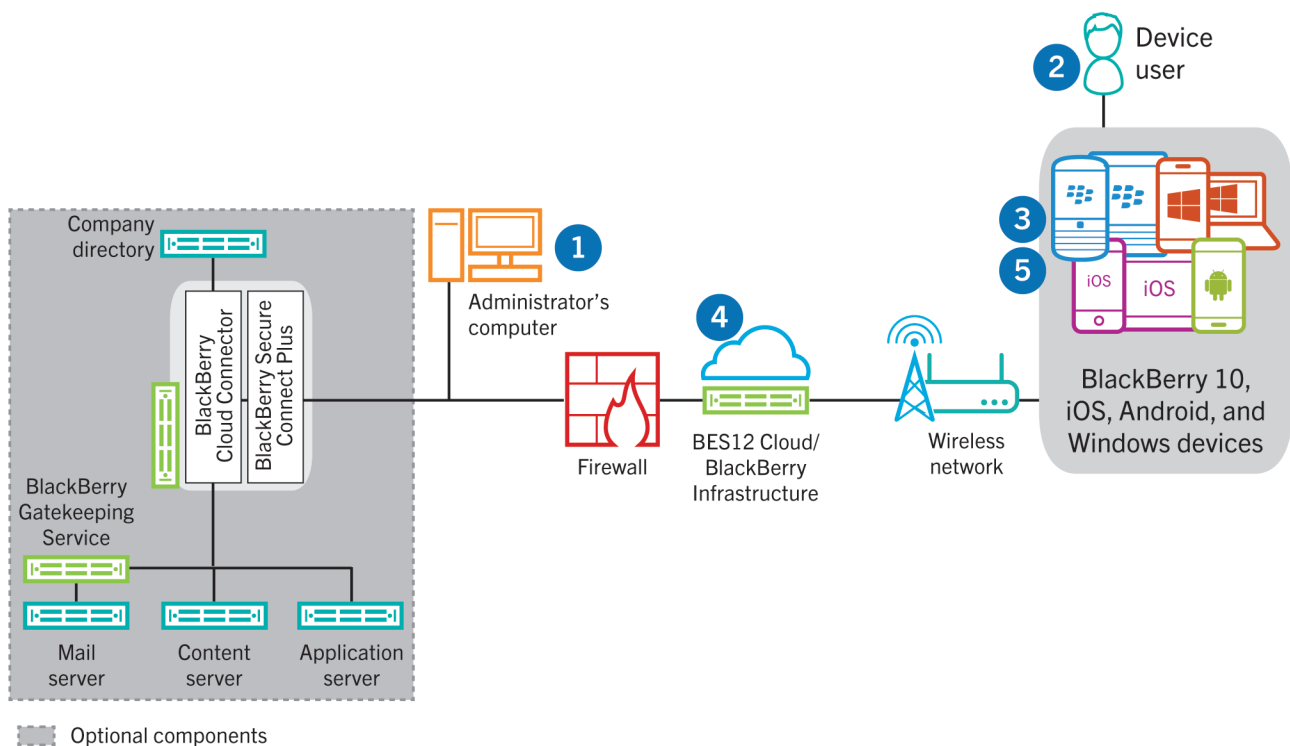
Component	Description
	If you activate the device using the Work and personal - full control (Samsung KNOX) activation type, you can manage aspects of the personal space using IT policy rules.
BES12 Client	<p>The BES12 Client connects to BES12 to receive management commands.</p> <p>The BES12 Client is located in the personal space.</p> <p>The BES12 Client also connects to the KLM Agent app on the device to verify the Samsung KNOX license.</p>
Workspace	<p>The workspace is created when you activate the device on BES12 using a Samsung KNOX activation type. It includes the following apps:</p> <ul style="list-style-type: none"> <li>• Email, contacts, and calendar apps connect to your mail server.</li> <li>• Google Play app connects to the Google Play store so that users can download and install work apps.</li> <li>• Samsung KNOX Apps store connects to the KNOX Marketplace so that users can download and install work apps that are only available to KNOX Workspace devices.</li> <li>• Work apps connect to your organization's network to access data.</li> </ul>
BlackBerry Infrastructure	The BlackBerry Infrastructure registers user information for device activation and management.
BES12 Cloud	BES12 Cloud is the EMM solution by BlackBerry that you can use to manage KNOX Workspace devices.

# Activating devices

Depending on the device type and the activation type that you specify for it, the device and BES12 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 ["Device activation" in the Administration content](#).

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 ["Creating activation profiles" in the Administration content](#).

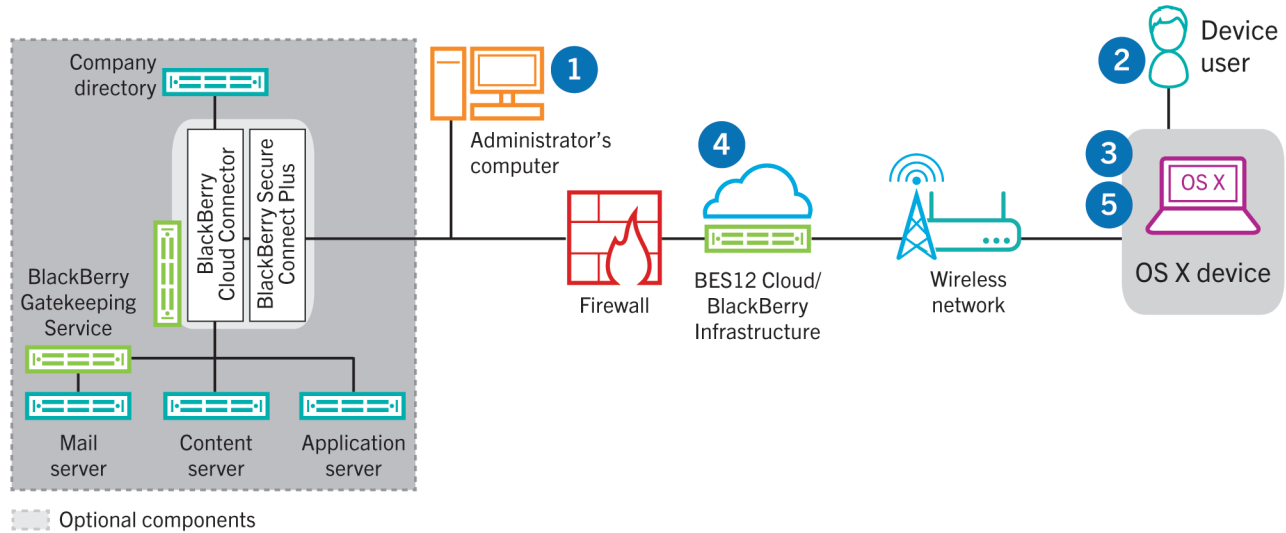
## Data flow: Activating a BlackBerry 10, iOS, Android, or Windows device



1. You perform the following actions:
  - a. Add a user to BES12 Cloud as a local user account or, if you installed the BlackBerry Cloud Connector, using the account information retrieved from your company directory.

- b** Assign an activation profile to the user.
  - c** If the user is activating a device to use Android for Work, configure BES12 Cloud to connect to your Google domain.
  - d** 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 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.
    - Communicate the BES12 Self-Service address to the user so that they can set their own activation password.
- 2.** The user performs the following actions:
- a** Downloads and installs the BES12 Client on an Android or a Windows Phone device, or the Good for BES12 app on an iOS device.
  - b** Enters their activation username and password on their device.
- 3.** The device sends an activation request to BES12.
- 4.** BES12 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 BES12 Cloud and completes the configuration. The device then sends confirmation to BES12 Cloud that the activation was successful.

## Data flow: Activating an OS X device

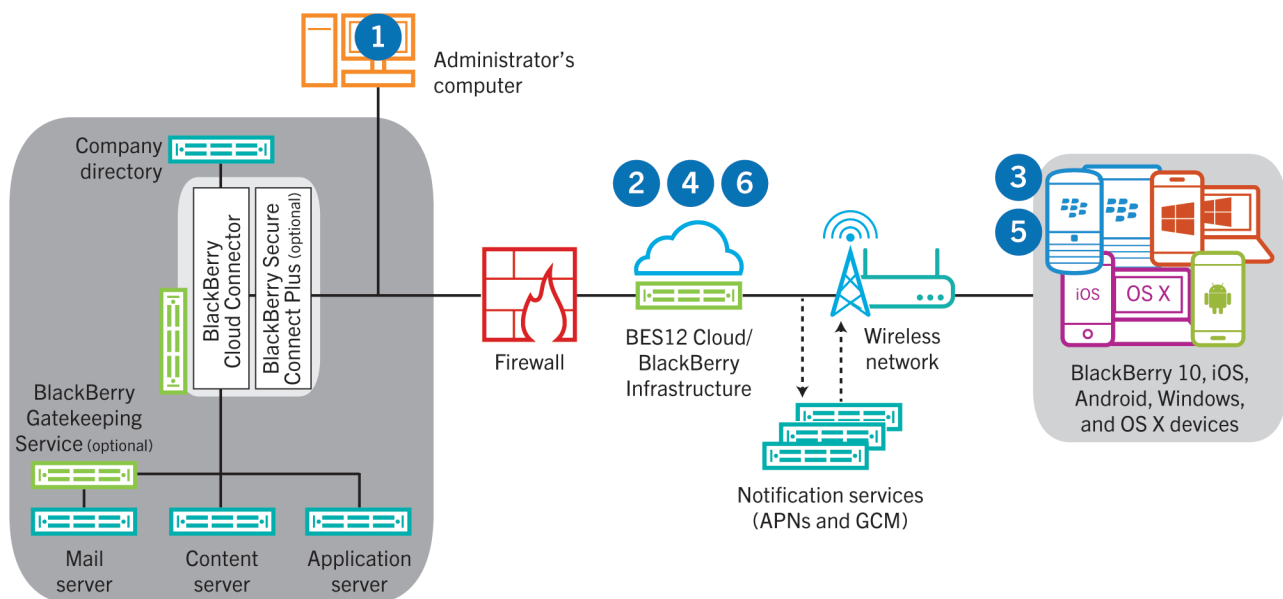


1. You perform the following actions:
  - a Add the user to BES12 Cloud as a local user account or, if you installed the BlackBerry Cloud Connector, using the account information retrieved from your company directory.
  - b Assign an activation profile to the user.
  - c Make sure that the user has the login information for BES12 Self-Service, including:
    - Web address for BES12 Self-Service
    - Username and password
    - Domain name
2. The user logs in to BES12 Self-Service on their OS X device and activates the device.
3. The device sends an activation request to BES12 Cloud.
4. BES12 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 BES12 Cloud and completes the configuration. The device then sends confirmation to BES12 Cloud that the activation was successful.

# 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, BES12 Cloud notifies the device that a configuration update is pending. Devices also poll BES12 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. Windows Phone 8.0 devices don't receive update notifications. Instead, these devices poll BES12 Cloud every hour to request pending updates.



---- iOS, Android, or Windows notification traffic

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. BES12 Cloud assigns the update and identifies the objects that must be shared with the device then performs one of the following actions:

- For BlackBerry 10 devices, BES12 Cloud notifies the Enterprise Management Agent on the device that an update is pending.
  - For Android devices, BES12 Cloud notifies the BES12 Client on the device that an update is pending using the GCM. The GCM sends a notification to the device to contact BES12 Cloud.
  - For iOS and OS X devices, BES12 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 BES12 Cloud.
  - For Windows Phone 8.1 and Windows 10 devices, BES12 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 BES12 Cloud.
  - For Windows Phone 8.0 devices, the device polls BES12 for updates at regular intervals.
- 3.** The device contacts BES12 Cloud to request any pending actions that must be performed on the device.
  - 4.** BES12 Cloud replies with the highest priority action.

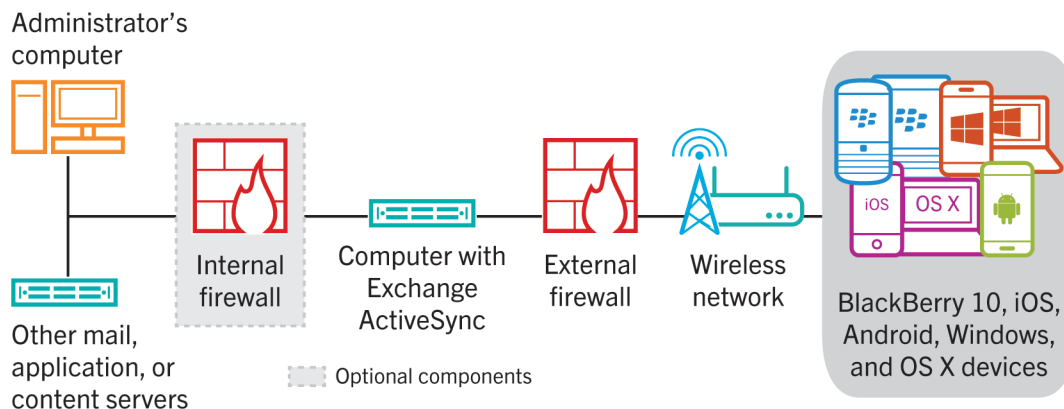
Priority is given to IT administration commands, such Lock device, followed by requests for device information, installed apps, and so on. BES12 Cloud sends one command at a time. If necessary, additional information is included in the response.
  - 5.** The device performs the following actions:
    - a** Inspects the response from BES12 Cloud
    - b** Schedules the command to be processed, and waits for the command to run
    - c** Sends a response to BES12 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, BES12 Cloud replies with the highest priority action. Steps 4 to 6 repeat until no more pending actions or commands must be performed and BES12 Cloud replies with an idle command.

# Sending and receiving work data

When users send and receive work data on a device, data can flow using the following connections:

- A direct connection from the device to the mail, content, or application server, for example an Exchange ActiveSync server, which is placed in a DMZ or is exposed to the public network
- Your organization's VPN or work Wi-Fi network to establish a direct connection 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 BlackBerry Secure Connect Plus, you can provide a secure IP tunnel through the BlackBerry Infrastructure between apps on BlackBerry 10, Samsung KNOX Workspace, Android for Work, and iOS devices with MDM controls activations and your organization's network.

This diagram shows a direct connection from the device to a computer that is running Exchange ActiveSync and is placed in a DMZ.

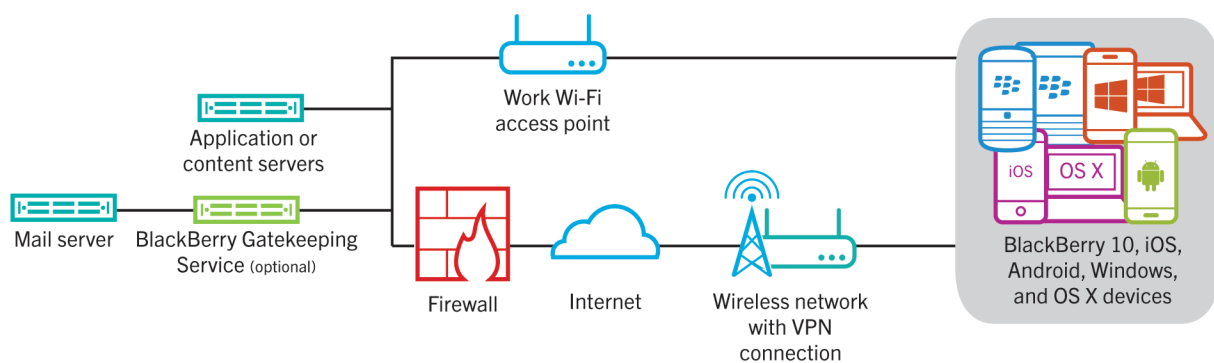




## Using your organization's VPN or work Wi-Fi network

Devices that have VPN or Wi-Fi profiles configured by you or by 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 a Windows Phone 8.1 device or an Android device that does not use Samsung KNOX Workspace must manually configure a VPN profile on their devices.

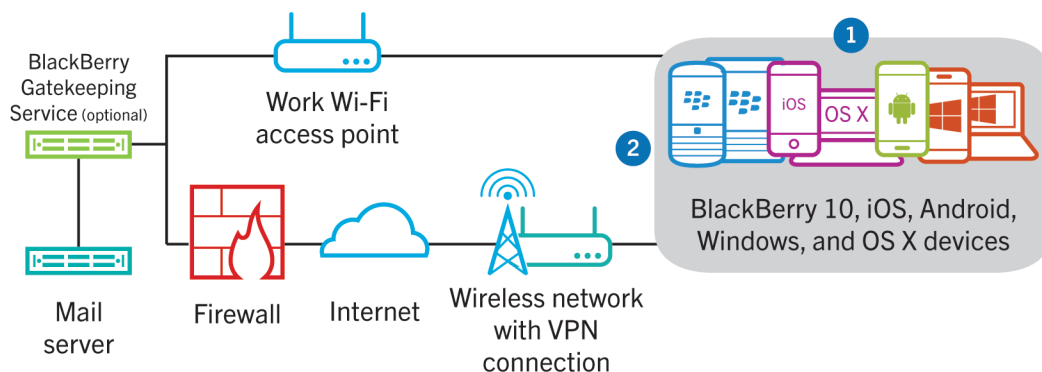
This diagram shows how data can travel when a device connects to your organization's resources using your organization's VPN or work Wi-Fi network.



All devices can use VPN or work Wi-Fi to send and receive Exchange ActiveSync data and other work data updates. If you enable BlackBerry Secure Connect Plus, BlackBerry 10, Samsung KNOX Workspace, Android for Work, and iOS devices with MDM controls activations use BlackBerry Secure Connect Plus when work VPN or work Wi-Fi connections aren't available.

## Data flow: Sending email from a device

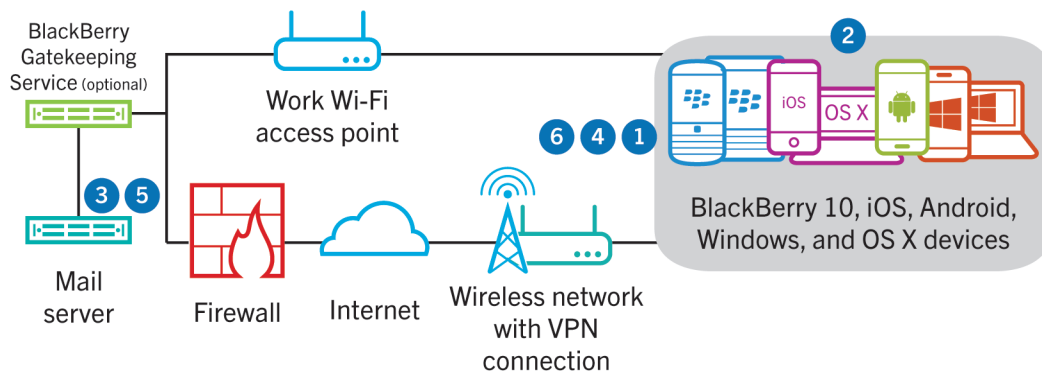
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



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

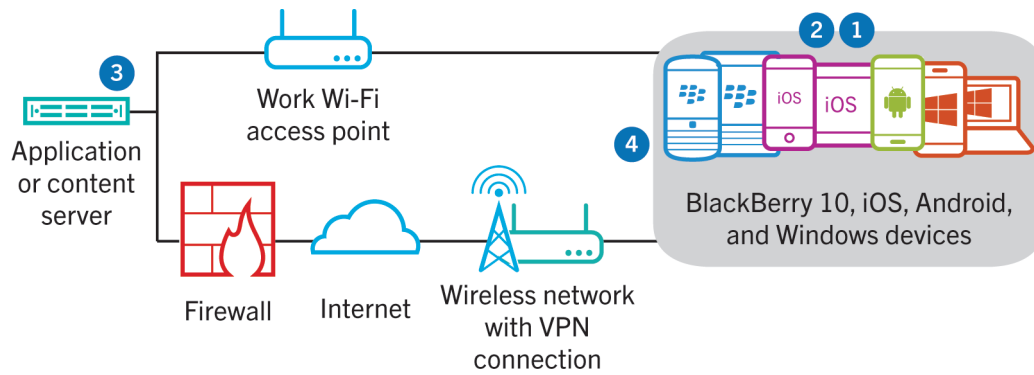
This data flow describes how work email and calendar data travels from the device to the mail server over your organization's VPN or work Wi-Fi network using Exchange ActiveSync.



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 "HTTP 200 OK" message to the device.
6. The device issues a new request and the process starts over.

## Data flow: Accessing an application or content server

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 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 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.

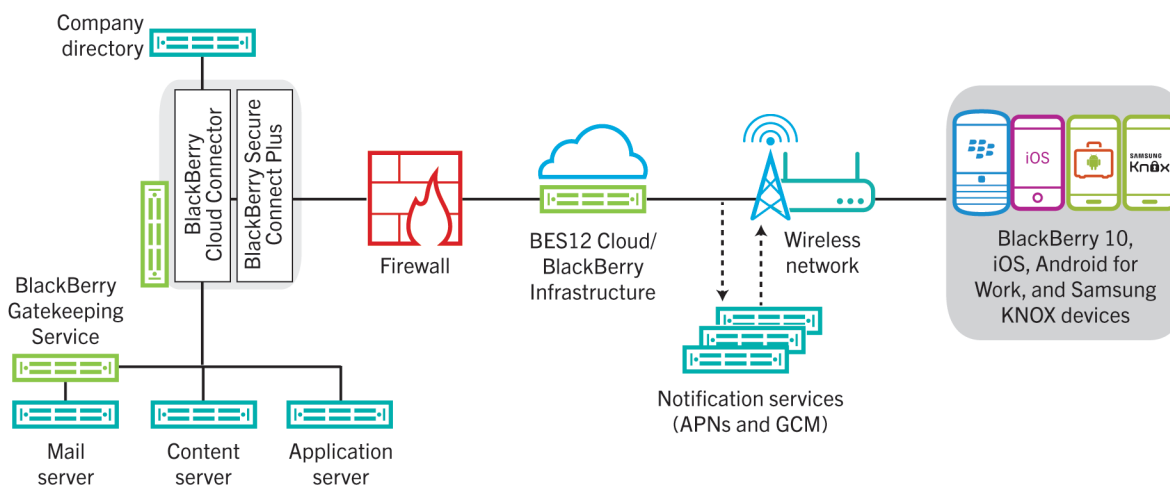
## Using BES12 Cloud and the BlackBerry Infrastructure

If you enable BlackBerry Secure Connect Plus, devices can connect to your organization's resources through BES12 Cloud to send and receive work data. BlackBerry 10 devices, iOS devices with the MDM controls activation type, and Android devices activated to use Android for Work or Samsung KNOX Workspace support BlackBerry Secure Connect Plus. BlackBerry Secure Connect Plus is installed when you install the BlackBerry Cloud Connector.

BlackBerry Secure Connect Plus provides a secure IP tunnel through the BlackBerry Infrastructure to transfer data between apps and your organization's network. One tunnel is established for each device, and the tunnel supports standard IPv4 protocols (TCP and UDP). When the tunnel is no longer required (for example, the user is in range of the work Wi-Fi network), it is terminated.

For BlackBerry 10, KNOX Workspace, and Android for Work devices, BlackBerry Secure Connect Plus provides a secure tunnel between all work space apps and your organization's network. For iOS devices with MDM controls activations, BlackBerry Secure Connect Plus can provide a secure tunnel between your organization's network and all apps or only specified apps using per-app VPN.

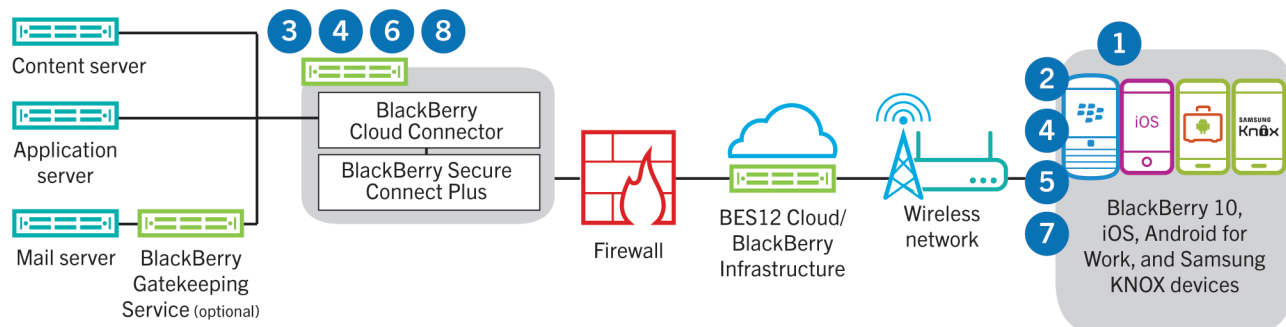
The following diagram shows how devices connect to your organization's resources using BlackBerry Secure Connect Plus.



For more information on how to turn on BlackBerry Secure Connect Plus using the enterprise connectivity profile, [see the Administration content](#).

## 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.



1. The user opens an app to access work data from a content or application server behind your organization's firewall.
  - On BlackBerry 10, Samsung KNOX Workspace, and Android for Work 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.
2. 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.
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.

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.



# Administrators

## Send an email to users

You can send an email to one or more users directly from the management console. The users must have an email address associated with their account.

**Before you begin:** To send an email to multiple users, you must be assigned an administrative role that has the "Send email to users" permission.

1. On the menu bar, click **Users**.
2. Perform one of the following tasks:

Task	Steps
Send an email to one user	<ol style="list-style-type: none"> <li>1. Search for a user account.</li> <li>2. In the search results, click the name of the user account.</li> <li>3. Click .</li> <li>4. Optionally, click <b>CC</b> and enter one or more email addresses (separated by commas or semicolons) to copy the email to yourself or others.</li> </ol>
Send an email to multiple users	<ol style="list-style-type: none"> <li>1. Select the check box for each user that you want to send an email to.</li> <li>2. Click .</li> <li>3. Optionally, click <b>To</b> or <b>CC</b> and enter one or more email addresses (separated by commas or semicolons) to send or copy the email to yourself or others.</li> </ol>

3. Enter a subject and message.
4. Click **Send**.

## Set an expiry time for commands

When you send the "Delete all device data" or "Delete only work data" command to a device, the device must connect to BES12 for the command to complete. If the device is unable to connect to BES12, the command remains in pending status and the device is not removed from BES12 unless you manually remove it. Alternatively, you can configure BES12 to automatically remove devices when the commands do not complete after a specified amount of time.

1. On the menu bar, click **Settings > General settings > Delete command expiry**.
2. Select **Automatically remove the device if the command has not completed** for one or both of **Delete all device data command expiry** and **Delete only work data command expiry**.
3. In the **Remove device after** field, type the number of days after which the command expires and the device is automatically removed from BES12.
4. Click **Save**.

# Windows 10 apps

## Add a Windows 10 app to the app list


To add Windows 10 apps to the app list, you must manage your app catalog in the Windows Store for Business and then synchronize the apps to BES12. When new apps are added to your app catalog, you can synchronize the apps with BES12 right away or wait until BES12 synchronizes automatically. BES12 synchronizes the app catalog every 24 hours.

You can allow users to install offline or online apps from the Windows Store for Business app catalog. Offline apps are downloaded by BES12 when you synchronize with the app catalog. Using offline apps is recommended because all management of these apps can be performed from BES12, and users can install them without connecting to the Windows Store for Business. After the apps are installed, devices receive updates to the apps from the Windows Store.

Online apps are downloaded directly from the Windows Store for Business.

### Before you begin:

- Configure BES12 to synchronize with the Windows Store for Business. For instructions, [see the Configuration content](#).
- If you want users to be able to install online apps, you must synchronize your directory with Microsoft Azure Active Directory using Microsoft AzureAD Connect.

1. On the menu bar, click **Apps**.
2. Click .
3. Click **Windows Store > 10**.
4. Click **Synchronize apps**.

## Allowing users to install online apps

To allow users to install online apps, the user must exist in your Microsoft Azure directory, and the user's email address in BES12 must match the user's email address in Microsoft Azure AD. You can synchronize your directory to Microsoft Azure using Microsoft Azure AD Connect. For information on using Microsoft Azure AD Connect, refer to <https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/>.

## Configuring BES12 to synchronize with the Windows Store for Business

If you want to manage Windows 10 apps, you must configure BES12 to synchronize with the Windows Store for Business.



When you configure BES12 to synchronize with the Windows Store for Business, you perform the following actions:

Step	Action
1	Create and configure a Microsoft Azure account.
2	Get the Client ID, Client key, and OAuth 2.0 token endpoint.
3	Create an administrator for the Windows Store for Business.

## Steps to configure BES12 to synchronize with the Windows Store for Business

When you configure BES12 to synchronize with the Windows Store for Business, you perform the following actions:

Step	Action
1	Create and configure a Microsoft Azure account.
2	Get the Client ID, Client key, and OAuth 2.0 token endpoint.
3	Create an administrator for the Windows Store for Business.

## Create and configure a Microsoft Azure account

To manage Windows 10 apps in BES12, you must create a Microsoft Azure account and authenticate BES12 with Microsoft Azure.

### Before you begin:

- Specify the shared network location to store offline apps. For more information about the network share location, see [Specify the shared network location for storing internal apps in the Administration content](#).
- Log in to <https://azure.microsoft.com> using your Microsoft account. If you do not have a Microsoft account, click **Create a Microsoft account** to create one.
  - If you do not have a Microsoft Azure subscription, click **Sign up for Windows Azure** and fill in the required fields. Credit card information is required.
  - Create a Microsoft Azure active directory. Optionally, you can use the default directory, but creating a new directory is recommended so that you can set a new directory name.

- a. In the left pane, click **Active Directory**.
  - b. Click **New**.  
Select **App Services > Active Directory > Directory > Custom Create**.
  - c. Fill in the necessary fields.
  - d. Click the checkmark.
4. To add a virtual representation of BES12 in the Microsoft Azure directory, perform the following actions. Adding a virtual representation allows BES12 to authenticate with Microsoft Azure.
    - a. In the directory that you created, click **Applications**.
    - b. Click **Add**.
    - c. Click **Add an application my organization is developing**.
    - d. Enter a name for the application. For example, **BES12**.
    - e. Select **Web application and/or web API**.
    - f. In the **Sign-on URL** field, enter any valid URL. For example, `http://example`. This field is not used in BES12 but must be filled in Microsoft Azure.
    - g. In the **App ID URI** field, enter any valid URI. For example, `http://example`. This field is not used in BES12 but must be filled in Microsoft Azure.
    - h. Click the checkmark.

## Get the Client ID, Client key, and OAuth 2.0 token endpoint

**Before you begin:** [Create and configure a Microsoft Azure account](#).

1. In the Microsoft Azure console, click **Configure**.
2. Copy the Client ID.
3. In the BES12 management console, on the menu bar, click **Settings > App Management > Windows 10 apps** and paste the Client ID in the **Client ID** field.
4. In the Microsoft Azure console, in the **keys** section, select a duration in the **Select duration** drop-down list.
5. Click **Save**.
6. Copy the key.
7. In the BES12 management console, paste the key in the **Client key** field.
8. In the Microsoft Azure console, click **View endpoints**.

9. In the **Token Endpoint URL** field, copy the URL.
10. In the BES12 management console, paste the token endpoint URL in the **OAuth 2.0 token endpoint** field.
11. In the BES12 management console, click **Next**.

## Create an administrator for the Windows Store for Business

To manage Windows 10 apps on devices, you must create an app catalog in the Windows Store for Business and synchronize the apps with BES12. To create the catalog in the Windows Store for Business, you must create at least one administrator account to log in to the store.

**Before you begin:** [Create and configure a Microsoft Azure account](#).

1. Go to the Microsoft Azure directory and click **Users**.
2. Click **Add User**.
3. On the screen, enter the required user information.
4. Click the next arrow.
5. On the screen, enter the required user information.
6. In the **Role** dropdown list, select **Global Admin**.
7. Enter an alternated email address.
8. Click the next arrow.
9. On the screen, click **create**.
10. Copy the temporary password.
11. Click the checkmark.
12. Click **Applications**.
13. In the virtual representation of BES12, click **Assign** to assign the app to the user.

# BlackBerry Secure Connect Plus

## Using BlackBerry Secure Connect Plus for secure connections to work resources

BlackBerry Secure Connect Plus is a BES12 component that provides a secure IP tunnel between apps and your organization's network:

- For BlackBerry 10, Samsung KNOX Workspace, and Android for Work devices, all work space apps use the secure tunnel.
- For iOS devices, you can allow all apps to use the tunnel or specify apps using per-app VPN.

This tunnel gives users access to work resources behind your organization's firewall while ensuring the security of data using standard protocols and end-to-end encryption.

BlackBerry Secure Connect Plus and a supported device establish a secure IP tunnel when it is the best available option for connecting to the organization's network. If a device is assigned a Wi-Fi profile or VPN profile, and the device can access the work Wi-Fi network or VPN, the device uses those methods to connect to the network. If those options are not available (for example, if the user is not in range of the work Wi-Fi network), then BlackBerry Secure Connect Plus and the device establish a secure IP tunnel.

For iOS devices, if you configure per-app VPN for BlackBerry Secure Connect Plus, the configured apps always use a secure tunnel connection through BlackBerry Secure Connect Plus, even if the app can connect to the work Wi-Fi network or VPN specified in a Wi-Fi or VPN profile.

Supported devices communicate with BES12 to establish the secure tunnel through the BlackBerry Infrastructure. One tunnel is established for each device. The tunnel supports standard IPv4 protocols (TCP and UDP). As long as the tunnel is open, apps can access network resources. When the tunnel is no longer required (for example, the user is in range of the work Wi-Fi network), it is terminated.

BlackBerry Secure Connect Plus offers the following advantages:

- The IP traffic that is sent between devices and BES12 is encrypted end-to-end using AES256, ensuring the security of work data.
- BlackBerry Secure Connect Plus provides a secure, reliable connection to work resources when a device user cannot access the work Wi-Fi network or VPN.
- BlackBerry Secure Connect Plus is installed behind your organization's firewall, so data travels through a trusted zone that follows your organization's security standards.

For more information about how BlackBerry Secure Connect Plus transfers data to and from devices, [see the Architecture content](#).

# Steps to enable BlackBerry Secure Connect Plus

When you enable BlackBerry Secure Connect Plus, you perform the following actions:

Step	Action
1	Verify that your organization's BES12 domain meets the requirements to use BlackBerry Secure Connect Plus.
2	Install the BlackBerry Cloud Connector, or upgrade the BlackBerry Cloud Connector to the latest version.
3	Enable BlackBerry Secure Connect Plus in the Default enterprise connectivity profile or in a custom enterprise connectivity profile that you create.
4	Optionally, specify the DNS settings for the BES12 Secure Connect Plus app.
5	Assign the enterprise connectivity profile to <a href="#">users</a> and <a href="#">groups</a> .

## Server and device requirements

To use BlackBerry Secure Connect Plus, your organization's environment must meet the following requirements.

For the BES12 domain:

- Your organization's firewall must allow outbound connections over port 3101 to [<region>.turnb.bbsecure.com](#) and [<region>.bbsecure.com](#). If you configure BES12 to use a proxy server, verify that the proxy server allows connections over port 3101 to these subdomains. For more information about domains and IP addresses to use in your firewall configuration, visit <http://support.blackberry.com/kb> to read article KB36470.
- The BlackBerry Secure Connect Plus component must be running.
- By default, Android for Work devices are restricted from using BlackBerry Secure Connect Plus to connect to Google Play and underlying services (com.android.providers.media, com.android.vending, and com.google.android.apps.gcs). Google Play does not have proxy support. Android for Work devices use a direct connection over the Internet to Google Play.

These restrictions are configured in the Default enterprise connectivity profile and in any new enterprise connectivity profiles that you create. It is recommended to keep these restrictions in place. If you remove these restrictions, you must contact Google Play support for the firewall configuration required to allow connections to Google Play using BlackBerry Secure Connect Plus.

For supported devices:

Device	Requirements
BlackBerry 10	<ul style="list-style-type: none"> <li>BlackBerry 10 OS version 10.3.2 or later</li> <li>Any of the following activation types: <ul style="list-style-type: none"> <li>Work and personal - Corporate</li> <li>Work space only</li> <li>Work and personal - Regulated</li> </ul> </li> </ul>
Samsung KNOX Workspace	<ul style="list-style-type: none"> <li>Android 5.0 or later</li> <li>Samsung KNOX MDM 5.0 or later</li> <li>Samsung KNOX 2.3 or later</li> <li>Any of the following activation types: <ul style="list-style-type: none"> <li>Work space only (Samsung KNOX)</li> <li>Work and personal - full control (Samsung KNOX)</li> <li>Work and personal - user privacy (Samsung KNOX)</li> </ul> </li> </ul>
Android for Work	<ul style="list-style-type: none"> <li>Android 5.1 or later</li> <li>Any of the following activation types: <ul style="list-style-type: none"> <li>Work space only (Android for Work - Premium)</li> <li>Work and personal - user privacy (Android for Work - Premium)</li> </ul> </li> </ul>
iOS	<ul style="list-style-type: none"> <li>iOS 9 or later</li> <li>Devices must be activated using the Good for BES12 app, available from the App Store</li> <li>MDM controls activation type</li> </ul>

For more information about the licenses that are required to use BlackBerry Secure Connect Plus, [see the Licensing content](#).

## Installing or upgrading the BlackBerry Secure Connect Plus component

When you install the BlackBerry Cloud Connector for the first time, the setup process also installs the BlackBerry Secure Connect Plus component on the same computer. If you upgrade the BlackBerry Cloud Connector to the latest version and BlackBerry Secure Connect Plus is not installed, the upgrade process installs BlackBerry Secure Connect Plus. If BlackBerry Secure Connect Plus was installed previously, the process upgrades BlackBerry Secure Connect Plus to the latest version.

For instructions to install or upgrade the BlackBerry Cloud Connector, [see the Configuration content](#). You must activate the BlackBerry Cloud Connector before you can enable BlackBerry Secure Connect Plus.

You have the option to route the data that travels between BlackBerry Secure Connect Plus and the BlackBerry Infrastructure through the BlackBerry Router or a TCP proxy server (transparent or SOCKS v5). You can configure the proxy settings using the BlackBerry Cloud Connector management console (General settings > Proxy).

**Note:** If you specify proxy information that is not valid, BlackBerry Secure Connect Plus stops running and cannot restart. If this issue occurs, correct the proxy information and restart the BES12 - BlackBerry Secure Connect Plus service in the Windows Services.

## Enabling and configuring BlackBerry Secure Connect Plus

When you install the BlackBerry Cloud Connector to establish a secure connection with your organization's resources (for example, Microsoft Active Directory), you also install the BlackBerry Secure Connect Plus component. After you install and activate the BlackBerry Cloud Connector, you can enable BlackBerry Secure Connect Plus using an enterprise connectivity profile.

### Enable BlackBerry Secure Connect Plus

If you want to allow devices to use BlackBerry Secure Connect Plus, you must enable BlackBerry Secure Connect Plus in an enterprise connectivity profile and assign the profile to users and groups. By default, BlackBerry Secure Connect Plus is not enabled for BlackBerry 10 or supported Android and iOS devices. You can do one of the following:

- Enable BlackBerry Secure Connect Plus for supported device types in the Default enterprise connectivity profile. If a user account is not assigned a custom enterprise connectivity profile directly or through group membership, BES12 assigns the Default profile.
- Create a custom enterprise connectivity profile using the following instructions and assign it to users and groups.

When the enterprise connectivity profile is applied to the device after activation, BES12 sends the device the SCEP and VPN profiles that are required to use BlackBerry Secure Connect Plus. BES12 also installs the BES12 Secure Connect Plus app on the device (for Android for Work devices, the app is installed automatically from Google Play; for iOS devices, the app is installed automatically from the App Store). On BlackBerry 10 devices, the app is hidden and does not require user interaction.

1. In the management console, on the menu bar, click **Policies and Profiles**.
2. Click **+** beside **Enterprise connectivity**.
3. Perform any of the following tasks:

Task	Steps
Enable for BlackBerry 10 devices	<ol style="list-style-type: none"> <li>1. On the <b>BlackBerry</b> tab, select the <b>Enable BlackBerry Secure Connect Plus</b> check box.</li> </ol>

Task	Steps
	<ol style="list-style-type: none"> <li data-bbox="610 275 1419 369">2. If you want to route secure tunnel traffic from BlackBerry 10 devices to the work network through a proxy server, in the <b>Proxy profile</b> drop-down list, select the appropriate proxy profile.</li> </ol>
Enable for supported Android devices	<ol style="list-style-type: none"> <li data-bbox="610 422 1419 474">1. On the <b>Android</b> tab, select the <b>Enable BlackBerry Secure Connect Plus</b> check box.</li> <li data-bbox="610 495 1419 695">2. If you want to route secure tunnel traffic from devices running Samsung KNOX 2.5 or later to the work network through a proxy server, in the <b>Proxy profile</b> drop-down list, select the appropriate proxy profile.  <b>Note:</b> The proxy profile setting does not apply to Android for Work devices or devices with Samsung KNOX version 2.4 or earlier.</li> <li data-bbox="610 726 1419 1157">3. If you want to restrict a specific work space app on Android for Work devices from using BlackBerry Secure Connect Plus, in the <b>Enterprise connectivity for Android for Work container</b> section, click <b>+</b> and type the app package ID. Repeat as necessary to restrict additional apps.  <b>Note:</b> By default, Google Play and underlying services (com.android.providers.media, com.android.vending, and com.google.android.apps.gcs) are restricted, as Google Play does not have proxy support. It is recommended to keep these restrictions in place. If you remove any of these restrictions, you must contact Google Play support for the firewall configuration required to allow connections to Google Play using BlackBerry Secure Connect Plus.</li> </ol>
Enable for iOS devices	<ol style="list-style-type: none"> <li data-bbox="610 1230 1419 1283">1. On the <b>iOS</b> tab, select the <b>Enable BlackBerry Secure Connect Plus</b> check box.</li> <li data-bbox="610 1304 1419 1503">2. If you want to configure per-app VPN so that only specific apps can use BlackBerry Secure Connect Plus, select the <b>Enable per-app VPN</b> check box. To specify the domains that are allowed to start a VPN connection in Safari, click <b>+</b>. If you want apps to be able to start the VPN connection automatically, select the <b>Allow apps to connect automatically</b> check box.</li> <li data-bbox="610 1514 1419 1808">3. If you want to allow all apps to use BlackBerry Secure Connect Plus, clear the <b>Enable per-app VPN</b> check box.  <b>Note:</b> If you select this option, users must manually turn on the VPN connection on their device to use BlackBerry Secure Connect Plus. As long as the VPN connection is on, the device uses BlackBerry Secure Connect Plus to connect to the work network. The user must turn the VPN connection off to use another connection, such as the work Wi-Fi network. Instruct users when it is appropriate to turn on and turn off the VPN connection (for</li> </ol>



Task	Steps
	<p>example, you can instruct users to turn on the VPN connection when they are not in range of the work Wi-Fi network).</p> <p><b>4.</b> If you want to specify rules for BlackBerry Secure Connect Plus connections, click <b>Enable VPN on demand</b> and specify the appropriate domains or host names, On Demand actions, and On Demand rules. For more information about these settings, see <a href="#">iOS and OS X: VPN profile settings</a>.</p> <p><b>Note:</b> If you allow all apps on iOS devices to use BlackBerry Secure Connect Plus, avoid adding On Demand rules such as Connect that attempt to create an “always on” VPN connection. If you do, during the activation process the device may try to establish a VPN connection before receiving the necessary profiles and certificates from BES12. As a result, the device cannot connect and the user must toggle the VPN connection to resolve the issue. It is recommended to instead use On Demand rules such as EvaluateConnection, which allow the device to receive the necessary profiles and certificates before attempting a VPN connection to specified domains.</p>

Currently, specifying a proxy profile on the iOS tab does not apply to BlackBerry Secure Connect Plus due to a known issue in the iOS software.

4. Click **Add**.
5. Assign the profile to groups or user accounts.
6. If you configured per-app VPN for iOS devices, when you assign an app or app group, associate it with the appropriate enterprise connectivity profile.

On Samsung KNOX Workspace and Android for Work devices, the BES12 Secure Connect Plus app prompts users to allow it to run as a VPN and to allow access to private keys on the device. Instruct users to accept the requests. Samsung KNOX Workspace, Android for Work, and iOS device users can open the app to view the status of the connection. No further action is required from users.

**After you finish:**

- If you created more than one enterprise connectivity profile, rank the profiles.
- If you are troubleshooting a connection issue with a KNOX Workspace, Android for Work, or iOS device, the app allows the user to send the device logs to an administrator's email address (the user enters an email address that you must provide). Note that the logs are not viewable with Winzip. It is recommended to use another utility such as 7-Zip.

## Specify the DNS settings for the BES12 Secure Connect Plus app


You can specify the DNS servers that you want the BES12 Secure Connect Plus app to use for secure tunnel connections. You can also specify DNS search suffixes. If you do not specify DNS settings, the app obtains DNS addresses from the computer that hosts the BlackBerry Secure Connect Plus component, and the default search suffix is the DNS domain of that computer.

1. In the BlackBerry Cloud Connector management console, in the left pane, click **General settings > BlackBerry Secure Connect Plus**.
2. Select the **Manually configure DNS servers** check box and click **+**.
3. Type the DNS server address in dot-decimal notation (for example, 192.0.2.0). Click **Add**.
4. If necessary, repeat steps 2 and 3 to add more DNS servers. In the **DNS servers** table, click the arrows in the **Ranking** column to set the priority for the DNS servers.
5. If you want to specify DNS search suffixes, complete the following steps:
  - a. Select the **Manage DNS search suffixes manually** check box and click **+**.
  - b. Type the DNS search suffix (for example, domain.com). Click **Add**.
6. If necessary, repeat step 5 to add more DNS search suffixes. In the **DNS search suffix** table, click the arrows in the **Ranking** column to set the priority for the DNS servers.
7. Click **Save**.

## Direct BlackBerry 10 work space traffic through BlackBerry Secure Connect Plus when a Wi-Fi network is available

If you use BES12 to configure a Wi-Fi profile and assign it to BlackBerry 10 devices, the devices prioritize the work Wi-Fi network above BlackBerry Secure Connect Plus. If the work Wi-Fi network is not available, and devices are not assigned a VPN profile or cannot access the VPN, devices use BlackBerry Secure Connect Plus. You have the option of directing all work space traffic through BlackBerry Secure Connect Plus even when devices can access the work Wi-Fi network. You may choose to use this option if your organization's security standards prevent device connections to work resources over the Wi-Fi network.

**Note:** Enabling this feature directs all work space traffic that would typically use the work Wi-Fi network through a secure connection to the BlackBerry Infrastructure. This feature may have an impact on your organization's data usage and network costs. Verify that this is your organization's preferred configuration before you enable this feature.

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand **Wi-Fi** and click the Wi-Fi profile that is assigned to BlackBerry 10 device users.
3. Click .
4. On the **BlackBerry** tab, in the **Associated profiles** section, select the **Use an enterprise connectivity profile with a BlackBerry Secure Connect Plus connection for work data** check box.
5. Click **Save**.

**After you finish:** If you created and assigned multiple Wi-Fi profiles, repeat this task as necessary.

# Integrating BES12 with your organization's PKI software

If your organization uses Entrust software or OpenTrust software to provide PKI services, you can extend certificate-based authentication to the devices that you manage with BES12.

Entrust products (such as Entrust IdentityGuard and Entrust Authority Administration Services) and OpenTrust products (such as OpenTrust PKI and OpenTrust CMS) issue client certificates. You can configure a connection with your organization's PKI software and use profiles to send the CA certificate and client certificates to devices.

## Connect BES12 to your organization's OpenTrust software

To extend OpenTrust certificate-based authentication to devices, you must add a connection to your organization's OpenTrust software. BES12 supports integration with OpenTrust PKI 4.8.0 and later and OpenTrust CMS 2.0.4 and later.

**Before you begin:** Contact your organization's OpenTrust administrator to obtain the URL of the OpenTrust server, the client-side certificate that contains the private key (.pfx or .p12 format), and the certificate password.

1. On the menu bar, click **Settings**.
2. Click **External integration > Certification authority**.
3. Click **Add an OpenTrust connection**.
4. In the **Connection name** field, type a name for the connection.
5. In the **URL** field, type the URL of the OpenTrust software.
6. Click **Browse**. Navigate to and select the client-side certificate that BES12 can use to authenticate the connection to the OpenTrust server.
7. In the **Certificate password** field, type the password for the OpenTrust server certificate.
8. To test the connection, click **Test connection**.
9. Click **Save**.

**After you finish:**

- When you use the BES12 connection with OpenTrust software to distribute certificates to devices, there may be a short delay before the certificates are valid. This delay might cause issues with email authentication during the device activation process. To resolve this issue, in the OpenTrust software, configure the OpenTrust CA and set "Backdate Certificates (seconds)" to 180.
- To edit a connection, click the connection name.
- To remove a connection, click ✕.

# Using Exchange Gatekeeping

Your organization can use the BlackBerry Gatekeeping Service to control which devices can access Exchange ActiveSync. For instructions for configuring Exchange ActiveSync and the BlackBerry Gatekeeping Service, in the [Configuration content](#), see [Controlling which devices can access Exchange ActiveSync](#).

When your organization uses the BlackBerry Gatekeeping Service, any device that is not whitelisted for Microsoft Exchange is reported in the BES12 Restricted Exchange ActiveSync devices list.

If you add a user account and assign the user account an email profile that has the BlackBerry Gatekeeping Service configured, all previously blocked, quarantined, or manually allowed devices related to the user account appear in the Restricted Exchange ActiveSync devices list.

If BES12 cannot obtain an Exchange ActiveSync ID from a device, it is not added to the allowed list for Microsoft Exchange. You can manually add these devices to the allowed list from the Restricted Exchange ActiveSync devices list. For example, if an Android device is activated without Secure Work Space using the MDM activation type, BES12 is not able to obtain an Exchange ActiveSync ID and you must manually whitelist the device in the Restricted Exchange ActiveSync devices list.

## Controlling which devices can access Exchange ActiveSync

You can stop unauthorized devices from using Exchange ActiveSync unless they are explicitly added to the allowed list. Devices that are not on the allowed list cannot access work email and organizer data. Using the BlackBerry Gatekeeping Service makes it easier to add devices to the allowed list.

To use the BlackBerry Gatekeeping Service, you must create a gatekeeping configuration for Microsoft Exchange Server or Microsoft Office 365 and assign an email profile to users that has the automatic gatekeeping server selected.

After you configure gatekeeping and assign the email profile to users, the users' devices are automatically added to the allowed list. If the email profile is removed from a user, the user's device is removed from the allowed list and can no longer connect to Microsoft Exchange (unless it is allowed using other means, for example, Windows PowerShell).

See the [Administration content](#) for more information about:

- [Adding an automatic gatekeeping server to an email profile](#)
- [Allowing or blocking devices that are not automatically added to the allowed list](#)

# Steps to configure Exchange ActiveSync and the BlackBerry Gatekeeping Service

When you configure the BlackBerry Gatekeeping Service, you perform the following actions:

Step	Action
1	Configure permissions for gatekeeping.
2	Allow only authorized devices to access Exchange ActiveSync.
3	Configure Microsoft IIS permissions for gatekeeping.
4	Create a gatekeeping configuration.
5	Create an email profile that has an automatic gatekeeping server selected and assign it to user accounts, user groups, or device groups. For instructions, <a href="#">see Create an email profile in the Administration content</a> .

## Configure permissions for gatekeeping

To use Exchange ActiveSync gatekeeping, you must create a user account in Microsoft Exchange Server or Microsoft Office 365 and give it the necessary permissions for gatekeeping.

If you are using Microsoft Office 365, create a Microsoft Office 365 user account and assign it the Mail Recipients and Organization Client Access roles.

If you are using Microsoft Exchange Server 2010 or later, follow the instructions below to configure management roles with the correct permissions to manage mailboxes and client access for Exchange ActiveSync. To perform this task, you must be a Microsoft Exchange administrator with the appropriate permissions to create and change management roles.

### Before you begin:

- On the computer that hosts Microsoft Exchange, create an account and mailbox to manage gatekeeping in BES12 (for example, BES12Admin). You must specify the login information for this account when you create an Exchange ActiveSync configuration. Note the name of this account, you will specify it at the end of the task below.
- WinRM must be configured with the default settings on the computer that hosts the Microsoft Exchange Server that you configure for gatekeeping. You must run the command `winrm quickconfig` from a command prompt as an administrator. When the tool displays `Make these changes [y/n]`, type `y`. After the command is successful, you see the following message.

```
WinRM has been updated for remote management.
```

```
WinRM service type changed to delayed auto start.
```

```
WinRM service started.
```

```
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP
```

on this  
machine.

1. Open the Microsoft Exchange Management Shell.
2. Type **New-ManagementRole -Name "<name\_new\_role\_mail\_recipients>" -Parent "Mail Recipients"**. Press ENTER.
3. Type **New-ManagementRole -Name "<name\_new\_role\_org\_ca>" -Parent "Organization Client Access"**. Press ENTER.
4. Type **New-ManagementRole -Name "<name\_new\_role\_exchange\_servers>" -Parent "Exchange Servers"**. Press ENTER.
5. Type **Get-ManagementRoleEntry "<name\_new\_role\_mail\_recipients>\" | Where {\$\_.Name -ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry**. Press ENTER.
6. Type **Get-ManagementRoleEntry "<name\_new\_role\_org\_ca>\" | Where {\$\_.Name -ne "Get-CasMailbox"} | Remove-ManagementRoleEntry**. Press ENTER.
7. Type **Get-ManagementRoleEntry "<name\_new\_role\_exchange\_servers>\" | Where {\$\_.Name -ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry**. Press ENTER.
8. Type **Add-ManagementRoleEntry "<name\_new\_role\_mail\_recipients>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox**. Press ENTER.
9. Type **Add-ManagementRoleEntry "<name\_new\_role\_mail\_recipients>\Get-ActiveSyncDevice" -Parameters Identity**. Press ENTER.
10. Perform this step only if you are using Microsoft Exchange 2013. Type **Add-ManagementRoleEntry "<name\_new\_role\_mail\_recipients>\Get-MobileDeviceStatistics" -Parameters Mailbox**. Press ENTER.
11. Perform this step only if you are using Microsoft Exchange 2013. Type **Add-ManagementRoleEntry "<name\_new\_role\_mail\_recipients>\Get-MobileDevice" -Parameters Mailbox**. Press ENTER.
12. Type **Add-ManagementRoleEntry "<name\_new\_role\_org\_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs**. Press ENTER.
13. Type **New-RoleGroup "<name\_new\_group>" -Roles "<name\_new\_role\_mail\_recipients>", "<name\_new\_role\_org\_ca>", "<name\_new\_role\_exchange\_servers>"**. Press ENTER.
14. Type **Add-RoleGroupMember -Identity "<name\_new\_group>" -Member "BES12Admin"**. Press ENTER.

## Allow only authorized devices to access Exchange ActiveSync

If your organization uses Microsoft Exchange Server 2010 or later, see [Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync](#).

If your organization uses Microsoft Office 365, see [Configure the mobile device access policy in Microsoft Office 365](#).

## Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync

You must configure Microsoft Exchange Server 2010 or later to allow only authorized devices to access Exchange ActiveSync. Devices for existing users that are not explicitly added to the allowed list in Microsoft Exchange must be quarantined until BES12 allows them access.

To perform this task, you must be a Microsoft Exchange administrator with the appropriate permissions to configure the `Set-ActiveSyncOrganizationSettings`. For information about how to allow only authorized devices to access Exchange ActiveSync, visit <https://technet.microsoft.com> to read article *Enable a Device for Exchange ActiveSync*.

**Before you begin:** Verify with your Microsoft Exchange administrator whether or not there are any users currently using Exchange ActiveSync.

If your organization's default access level for Exchange ActiveSync is set to allow, and you have users setup and successfully synchronizing their devices, you must make sure that these users have a personal exemption or device rule associated to their user account or device before you set the default access level to quarantine. If they do not, then they are quarantined and their devices do not synchronize until they are allowed by BES12.

For more information about setting the default access level for Exchange ActiveSync to quarantine, visit <http://support.blackberry.com/kb> to read article KB33531.

1. On a computer that hosts the Microsoft Exchange Management Shell, open the Microsoft Exchange Management Shell.
2. Type **Set-ActiveSyncOrganizationSettings –DefaultAccessLevel Quarantine**. Press ENTER.

## Configure the mobile device access policy in Microsoft Office 365

To use the BlackBerry Gatekeeping Service with Microsoft Office 365, you must configure the mobile device access policy in Microsoft Office 365 to quarantine devices by default.

1. Log in to the Microsoft Office 365 administration portal.
2. In the side menu, click **Admin**.
3. Click **Exchange**.
4. In the **Mobile** section, click **mobile device access**.
5. Click **Edit**.
6. Click **Quarantine - Let me decide to block or allow later**.

## Configure Microsoft IIS permissions for gatekeeping

BES12 uses Windows PowerShell commands to manage the list of allowed devices. To use the BlackBerry Gatekeeping Service, you must configure Microsoft IIS permissions. Perform the following actions on the computer that hosts the Microsoft client access server role.

1. Open the Microsoft Internet Information Services (IIS) Manager.



2. In the left pane, expand the server.
3. Expand **Sites > Default Web Site**.
4. Right-click the PowerShell folder. Select **Edit Permissions**.
5. Click the **Security** tab. Click **Edit**.
6. Click **Add** and enter the <new\_group> that was created when you configured the Microsoft Exchange permissions for gatekeeping.
7. Click **OK**.
8. Confirm that **Read & execute**, **List folder contents**, and **Read** are selected. Click **OK**.
9. Select the **PowerShell** folder. Double-click the **Authentication** icon.
10. Select **Windows Authentication**. Click **Enable**.
11. Close the Microsoft Internet Information Services (IIS) Manager.

## Create a gatekeeping configuration

You can create a gatekeeping configuration so that devices that comply with your organization's security policies can connect to the Microsoft Exchange Server or Microsoft Office 365.

### Before you begin:

- [Configure permissions for gatekeeping](#).
- [Allow only authorized devices to access Exchange ActiveSync](#).
- [Configure Microsoft IIS permissions for gatekeeping](#).

1. In the BlackBerry Cloud Connector management console, click **General settings > BlackBerry Gatekeeping Service**.
2. Click **+**.
3. In the **Server name** field, type the name of the Microsoft Exchange Server or Microsoft Office 365 environment that you want to manage access to.
4. Type the username and password for the account that you created to manage Exchange ActiveSync gatekeeping.
5. In the **Authentication type** drop-down list, select the type of authentication that is used for the Microsoft Exchange Server or Microsoft Office 365.
6. Select the **Use SSL** check box to enable SSL authentication between BES12 and the Microsoft Exchange Server or Microsoft Office 365. Optionally, select additional certificate checks.
7. In the **Proxy type** drop-down list, select the type of proxy configuration, if any, that is used between BES12 and the Microsoft Exchange Server or Microsoft Office 365.
8. If you selected a proxy configuration in the previous step, select the authentication type that is used on the proxy server.
9. If necessary, select **Authentication required** and type the username and password.
10. Click **Test Connection** to verify that the connection is successful.
11. Click **Save**.

**After you finish:** Create an email profile that has an automatic gatekeeping server selected and assign it to user accounts, user groups, or device groups. For instructions, see [Create an email profile in the Administration content](#).

## Allow a device to access Microsoft ActiveSync

You can manually allow a device to access Microsoft ActiveSync so that a user can receive email messages and other information from the Microsoft Exchange Server on the device.

**Before you begin:** Configure the BlackBerry Gatekeeping Service. In the [Configuration content](#), see [Controlling which devices can access Exchange ActiveSync](#).

1. On the menu bar, click **Users > Exchange gatekeeping**.
2. Search for a device.
3. In the **Action** column, click ✓.

## Block a device from accessing Microsoft ActiveSync

You can manually block a previously allowed device from accessing Microsoft ActiveSync. Blocking a device prevents a user from retrieving email messages and other information from the Microsoft Exchange Server on the device.

**Before you begin:** Configure the BlackBerry Gatekeeping Service. In the [Configuration content](#), see [Controlling which devices can access Exchange ActiveSync](#).

1. On the menu bar, click **Users**.
2. Click **Exchange gatekeeping**.
3. Search for a device.
4. In the **Action** column, click ⊘.

# Product documentation

Resource	Description
<b>Overview and what's new</b>	<ul style="list-style-type: none"> <li>• Introduction to BES12 and its features</li> <li>• What's new</li> </ul>
<b>Architecture and data flows</b>	<ul style="list-style-type: none"> <li>• Architecture</li> <li>• Descriptions of BES12 components</li> <li>• Descriptions of activation and other data flows, such as configuration updates and email, for different types of devices</li> </ul>
<b>Release notes and advisories</b>	<ul style="list-style-type: none"> <li>• Descriptions of fixed issues</li> <li>• Descriptions of known issues and potential workarounds</li> <li>• What's new</li> </ul>
<b>Licensing</b>	<ul style="list-style-type: none"> <li>• Instructions to obtain, activate, and manage licenses</li> <li>• Descriptions of different types of licenses</li> <li>• Instructions for activating and managing licenses</li> </ul>
<b>Configuration</b>	<ul style="list-style-type: none"> <li>• Instructions for how to configure server components before you start administering users and their devices</li> <li>• Instructions for migrating data from an existing BES10 or BES12 database</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Basic and advanced administration for all supported device types, including BlackBerry 10 devices, iOS devices, OS X computers, Android devices, Windows devices and BlackBerry OS (version 5.0 to 7.1) and earlier devices</li> <li>• Instructions for creating user accounts, groups, roles, and administrator accounts</li> <li>• Instructions for activating devices</li> <li>• Instructions for creating and assigning IT policies and profiles</li> <li>• Instructions for managing apps on devices</li> <li>• Descriptions of profile settings</li> <li>• Descriptions of IT policy rules for BlackBerry 10 devices, iOS devices, OS X computers, Android devices, Windows devices and BlackBerry OS (version 5.0 to 7.1) and earlier devices</li> </ul>

Resource	Description
<b>Security</b>	<ul style="list-style-type: none"><li>• Description of device security features</li><li>• Description of how you can use BES12 to manage device security features such as encryption, passwords, and data wiping</li><li>• Description of how BES12 protects your data in transit between devices, the BlackBerry Infrastructure, BES12, and your organization's resources</li></ul>
<b>Compatibility matrix</b>	<ul style="list-style-type: none"><li>• List of supported operating systems, database servers, browsers, and mobile operating systems for the BES12 server</li><li>• List of mail servers for BES12 Secure Work Space</li><li>• List of supported Samsung KNOX operating systems</li><li>• List of supported Android for Work operating systems</li><li>• List of mail servers for BlackBerry 10 OS</li></ul>

# Glossary

<b>AES</b>	Advanced Encryption Standard
<b>AET</b>	application enrollment token
<b>APNs</b>	Apple Push Notification service
<b>BES12</b>	BlackBerry Enterprise Service 12
<b>CA</b>	certification authority
<b>certificate</b>	A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that is stored separately. A certificate authority signs the certificate to indicate that it is authentic and can be trusted.
<b>CRL</b>	certificate revocation list
<b>DEP</b>	Device Enrollment Program
<b>DNS</b>	Domain Name System
<b>DPD</b>	Dead Peer Detection
<b>EAP</b>	Extensible Authentication Protocol
<b>EAP-FAST</b>	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling
<b>EAP-MS-CHAP</b>	Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol
<b>EAP-TLS</b>	Extensible Authentication Protocol Transport Layer Security
<b>EMM</b>	Enterprise Mobility Management
<b>FQDN</b>	fully qualified domain name
<b>GTC</b>	Generic Token Card
<b>HMAC</b>	keyed-hash message authentication code
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol over Secure Sockets Layer
<b>ICCID</b>	Integrated Circuit Card Identifier
<b>IKE</b>	Internet Key Exchange
<b>IMAP</b>	Internet Message Access Protocol
<b>IMEI</b>	International Mobile Equipment Identity
<b>IP</b>	Internet Protocol
<b>IPsec</b>	Internet Protocol Security
<b>IT policy</b>	An IT policy consists of various rules that control the security features and behavior of devices.
<b>LAN</b>	local area network
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MD5</b>	Message-Digest Algorithm, version 5

<b>MDM</b>	mobile device management
<b>MS-CHAP</b>	Microsoft Challenge Handshake Authentication Protocol
<b>NAT</b>	network address translation
<b>NTLM</b>	NT LAN Manager
<b>OCSP</b>	Online Certificate Status Protocol
<b>PAC</b>	proxy auto-configuration
<b>PFS</b>	Perfect Forward Secrecy
<b>PKI</b>	Public Key Infrastructure
<b>PMK</b>	pairwise master key
<b>POP</b>	Post Office Protocol
<b>PRF</b>	pseudorandom function family
<b>PSK</b>	pre-shared key
<b>SCEP</b>	simple certificate enrollment protocol
<b>SHA</b>	Secure Hash Algorithm
<b>SIM</b>	Subscriber Identity Module
<b>S/MIME</b>	Secure Multipurpose Internet Mail Extensions
<b>space</b>	A space is a distinct area of the device that enables the segregation and management of different types of data, applications, and network connections. Different spaces can have different rules for data storage, application permissions, and network routing. Spaces were formerly known as perimeters.
<b>SSL</b>	Secure Sockets Layer
<b>Supervised iOS devices</b>	Supervised devices are configured to allow additional control of iOS device features. To enable supervision of iOS devices that are owned by your organization, you can use Apple Configurator or the Device Enrollment Program.
<b>TCP</b>	Transmission Control Protocol
<b>TLS</b>	Transport Layer Security
<b>USB</b>	Universal Serial Bus
<b>VPN</b>	virtual private network
<b>xAuth</b>	Extended Authentication

# Legal notice

©2016 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BES, EMBLEM Design, ATHOC, EMBLEM Design, ATHOC & Design and PURPLE GLOBE Design, GOOD, GOOD WORK, LOCK Design, MANYME, MOVIRTU, SECUSMART, SECUSMART & Design, SECUSUITE, SECUVOICE, VIRTUAL SIM PLATFORM, WATCHDOX and WORKLIFE 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.

GOOD and EMBLEM Design 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.

Android, Google Chrome, and Google Play are trademarks of Google Inc. Apple, App Store, Apple Configurator, iCloud, OS X, and Safari are trademarks of Apple Inc. Aruba and VIA are trademarks of Aruba Networks, Inc. Bell is a trademark of Bell Canada. Bluetooth is a trademark of Bluetooth SIG. Check Point and VPN-1 are trademarks of Check Point Software Technologies Ltd. Cisco, Cisco AnyConnect, Cisco IOS, and PIX are trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. F5 is a trademark of F5 Networks, Inc. HTC EVO is a trademark of HTC Corporation. IBM, Domino, IBM Verse, and Notes are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Juniper is a trademark of Juniper Networks, Inc. Kerberos is a trademark of the Massachusetts Institute of Technology. Microsoft, Active Directory, ActiveSync, Windows, and Windows Phone are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. OpenVPN is a trademark of OpenVPN Technologies, Inc. PGP is a trademark of PGP Corporation. Pulse Secure is a trademark of Pulse Secure LLC. RSA is a trademark of RSA Security. SonicWALL and Mobile Connect are trademarks of Dell, Inc. Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries. T-Mobile is a trademark of Deutsche Telekom AG. Wi-Fi, WPA, and WPA2 are trademarks of the Wi-Fi Alliance. Entrust, Entrust IdentityGuard, and Entrust Authority Administration Services are trademarks of Entrust, Inc. KNOX and Samsung KNOX are trademarks of Samsung Electronics Co., Ltd. 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  
200 Bath Road  
Slough, Berkshire SL1 3XE  
United Kingdom

Published in Canada